



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 30, 2019

Ms. Emma Best

via email: 75437-46472565@requests.muckrock.com

RE: FOIA No. 2019-IGFP-00438

Dear Ms. Best:

This responds to your June 17 Freedom of Information Act (FOIA) request for records related to Records mentioning, describing, or generated as a result of 13 Computer – Theft of Identity investigations conducted by the OIG Office of Investigations (specific case numbers provided). On July 16, we received your follow up correspondence for status of your request. As explained in our July 17 email acknowledging receipt of your request, we could find no record of having received your original request and apologize for the delay.

As our FOIA program continues to evolve, we are encouraging requesters to submit requests, with all attachments, via email at foia@uspsoig.gov. Additionally, this speeds up our ability to conduct a search for responsive documents and issue our final determination. This also allows for more accurate searching as we can cut and paste information directly into search fields.

We reviewed the available Closing Memoranda, transmittal letters, and Reports of Investigation associated with the provided case numbers and determined the following:

- 02UIHQ0559S3CT, consisting of 8 pages: One page is appropriate for release without redaction, while the remaining 7 pages are appropriate for release with redactions made under FOIA Exemptions (b)(7)(c) and (b)(7)(e), 5 U.S.C. § 552 (b)(7)(c)¹ and (b)(7)(e)².
- 02UIHQ0639S3CT, consisting of 6 pages: All 6 pages are appropriate for release with redactions made under FOIA Exemptions (b)(3), (b)(7)(c), and (b)(7)(e), 5 U.S.C. § 552 (b)(3)³, (b)(7)(c) and (b)(7)(e).

¹ Exemption (7)(C) permits the withholding of records or information compiled for law enforcement purposes, the release of which could constitute an unwarranted invasion of the personal privacy of third parties. Lacking an individual's consent or an overriding public interest, third party investigatory records and/or allegations of misconduct must be withheld under Exemption (7)(C). This includes the names of, or identifying statements made by, any persons making allegations against the subject of an OIG investigation. The withheld material consists of third-party interviews which must be protected to provide the confidence necessary to encourage cooperation with law enforcement agencies. None of the information being withheld is appropriate for discretionary disclosure. The names of law enforcement personnel are among the items redacted based on 5 U.S.C. § 552(b)(7)(C).

² Exemption (7)(E) permits the withholding of records which would disclose techniques and procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations of prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. In addition, exemption (7)(E) permits the withholding of law enforcement guidelines that pertain to the prosecution or investigative stage of a law enforcement matter, to include law enforcement manuals, policy guidance documents, settlement guidelines, monographs, and emergency plans, as well as other types of law enforcement guidelines.

³ Exemption (b)(3) provides agencies may withhold records exempted from disclosure by another statute that "establishes particular criteria for withholding or refers to particular types of matters to be withheld." Under the

- 05UIMI4153S3IO, consisting of 6 pages: One page is appropriate for release without redaction, while the remaining 5 pages are appropriate for release with redactions made under FOIA Exemptions(b)(3), (b)(7)(c), and (b)(7)(e), 5 U.S.C. § 552 (b)(3), (b)(7)(c) and (b)(7)(e).
- 07UIBH0777CI3MS, consisting of 9 pages: Two pages are appropriate for release without redaction, while the remaining 7 pages are appropriate for release with redactions made under FOIA Exemptions (b)(3), (b)(6), and (b)(7)(c), 5 U.S.C. § 552 (b)(3), (b)(6)⁴, and (b)(7)(c).
- 07UIGR4325CI3MS, consisting of 3 pages: One page is appropriate for release without redaction, while the remaining 2 pages are appropriate for release with redactions made under FOIA Exemption (b)(7)(c), 5 U.S.C. § 552 (b)(7)(c).
- 08UICH4504GC04GC, consisting of 3 pages: All 3 pages are appropriate for release with redactions made under FOIA Exemption (b)(7)(c), 5 U.S.C. § 552 (b)(7)(c).
- 08UIIN7062GC04GC, consisting of 2 pages: Both pages are appropriate for release with redactions made under FOIA Exemptions (b)(7)(c), and (b)(7)(e), 5 U.S.C. § 552 (b)(7)(c) and (b)(7)(e).
- 08UINY3819GC04GC, consisting of 3 pages: All 3 pages are appropriate for release with redactions made under FOIA Exemption (b)(7)(c), 5 U.S.C. § 552 (b)(7)(c).
- 08UIRF3733GC04GC, consisting of 18 pages: Two pages are appropriate for release without redaction, while the remaining 16 pages are appropriate for release with redactions made under FOIA Exemption (b)(7)(c), 5 U.S.C. § 552 (b)(7)(c).
- 08UITA3531GC04GC, consisting of 8 pages: One page is appropriate for release without redaction, while the remaining 7 pages are appropriate for release with redactions made under FOIA Exemptions (b)(6) and (b)(7)(c), 5 U.S.C. § 552 (b)(6) and (b)(7)(c).
- 09UIBG2958GC04GC, consisting of 20 pages: Two pages are appropriate for release without redaction, while the remaining 18 pages are appropriate for release with redactions made under FOIA Exemptions (b)(3) and (b)(7)(c), 5 U.S.C. § 552 (b)(3) and (b)(7)(c).
- 09UISL0936GC04GC, consisting of 8 pages: One page is appropriate for release without redaction, while the remaining 7 pages are appropriate for release with

Inspector General Act of 1978, an OIG is duty bound to protect information provided by agency employees during an investigation. Public Law 95-452 5 U.S.C. app. 3 § 7(b).

⁴ Exemption (b)(6) pertains to information the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties. The withheld material includes names, titles, and identifying information of private citizens. This information is not appropriate for discretionary disclosure.


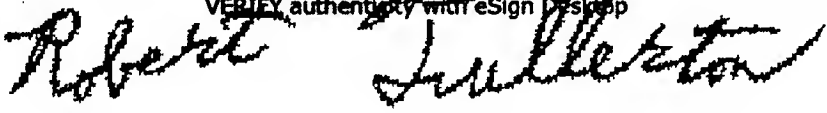
redactions made under FOIA Exemptions (b)(3) and (b)(7)(c), 5 U.S.C. § 552 (b)(3) and (b)(7)(c).

- 09UISL2419GC04GC, consisting of 1 page: This page is appropriate for release with redactions made under FOIA Exemption (b)(7)(c), 5 U.S.C. § 552 (b)(7)(c).

If you have questions regarding the processing of this request, you may contact me at 703-248-2410. You may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with our action on your FOIA request, you may file an administrative appeal. To do so, write to the attention of Gladis Griffith, Deputy General Counsel, 1735 N. Lynn Street, Arlington, VA 22209-2020, within 90 days of the date of this letter. We accept written appeals via U.S. Mail; e-mail to FOIA@uspsoig.gov; or fax to 703-248-4626. Include the initial request number (e.g., 20XX-IGXX-00XXX) and the date of this letter. Explain what specific action the FOIA Office took that you are appealing. Mark all correspondence "Freedom of Information Act Appeal."

Sincerely,

E-Signed by Fullerton, Robert
VERIFY authenticity with eSign Desktop 


Robert Fullerton
Manager – FOIA, Policy, and Records



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
1735 NORTH LYNN STREET
ARLINGTON, VA 22209-2020

DATE: December 11, 2003

PREPARED BY: (b)(7)(C)

CASE #: 02UIHQ0559S3CT

CROSS REFERENCE #:

TITLE: ONLINE FRAUD USING USPS WEBSERVER

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM May 20, 2002 TO December 12, 2003

LOCATION OF OFFENSE: USPS, INTERNET WEBSITE

STATUS OF CASE: CLOSED

- ☐ CONTINUING INVESTIGATION
- ☐ SIGNIFICANT DEVELOPMENT
- ☐ PROSECUTION REPORT
- ☐ PENDING JUDICIAL ACTION
- ☐ PENDING ADMINISTRATIVE ACTION
- ☐ PENDING OTHER ACTION
- ☐ REFERRAL TO ANOTHER AGENCY
- ☒ CLOSED

JOINT AGENCIES:

NONE

DISTRIBUTION:

USPSOIG

TABLE OF CONTENTS

- I. INTRODUCTION
- II. SYNOPSIS
- III. NARRATIVE
- IV. LAW ENFORCEMENT AND OTHER RECORDS
- V. JUDICIAL/ADMINISTRATIVE REFERRALS
- VI. STATUTES
- VII. SUBJECTS
- VIII. DISPOSITION OF EVIDENCE, CONTRABAND, AND PROPERTY
- IX. STATUS OF INVESTIGATION
- X. EXHIBITS

I. INTRODUCTION

This investigation was initiated on May 20, 2002 when information (incident 020502-003) provided by the U.S. Postal (USPS), Computer Incident Response Team (CIRT) revealed an alleged attempt to defraud American Online (AOL) customers via the use of a USPS computer system. This appeared to be in violation of 18 USC Chapter 47 § 1029, Fraud and related activity in connection with access devices and 18 USC 1343, wire fraud.

II. SYNOPSIS

This investigation concerned an allegation that the USPS website was being used to launch fraudulent Internet activity against AOL customers. The network connection associated with the fraudulent network activity was traced to an account owned by (b)(7)(C). Subsequent interviews in the neighborhood of (b)(7)(C) revealed he was suspected of using the stolen credit card accounts to send (b)(7)(C) flowers and threatening messages.

Investigative effort revealed the credit card of a U.S. Marine Corps (USMC) member was used to order flowers from two online flower companies. The flowers contained notes of a threatening nature. These flowers were sent to a Federal public housing manager in the Boston, MA area. The investigation developed two suspects in Newton, MA, (b)(7)(C). Both individuals are purportedly unemployed and skilled with computers. The Newton Police Department (NPD) reported that (b)(7)(C) is suspected of committing an armed robbery. (b)(7)(C) has been involved in several incidents of assault, property damage, and vandalism. Subpoenas were served on various online companies besides the flower companies. None of the returned records developed any evidence implicating (b)(7)(C) in the Internet fraud. This case is being closed because of this lack of evidence and no further logical investigative leads.

III. NARRATIVE

The CIRT referred this case to the USPS, Office of Inspector General (OIG) on May 20, 2002. The USPS website, www.usps.gov, was used as a vehicle to commit online fraud against America On Line (AOL) customers. A review of the CIRT incident report resulted in subpoenas being issued to AT&T and Hotmail. The review identified Internet Protocol (IP) address (b)(7)(C) as the source of the May 3, 2002 attack via the USPS website. As a result of the subpoena request AT&T officials revealed the source IP originated from an AT&T broadband account belonging to (b)(7)(C).

The review also identified email address (b)(7)(C) as being implicated in the fraudulent activity. An email was sent to the suspected perpetrator email address, (b)(7)(C) in an effort to gain information regarding the computer system used in this attack.

Background information gathered via (b)(7)(C), (b)(7)(E) disclosed that (b)(7)(C)

A confidential source (C-001) disclosed that (b)(7)(C) named, (b)(7)(C) who is "good with computers". A second interview of C-001 identified (b)(7)(C) as another possible suspect. The source described (b)(7)(C) as a good friend of (b)(7)(C) and competent with computers. Background information gathered via (b)(7)(C), on (b)(7)(C) confirmed that he resided at (b)(7)(C) the same address used by (b)(7)(C)

An interview of Detective (b)(7)(C) disclosed that (b)(7)(C) is suspected of committing armed robbery in the local area. On February 4, 2003, (b)(7)(C) was reinterviewed, he disclosed that (b)(7)(C) had a history of (b)(7)(C) in the (b)(7)(C) area.

On May 30, 2003, (b)(7)(C)

(b)(7)(C)

On June 19, 2003, with the assistance of the Naval Criminal Investigative Service (NCIS), (b)(7)(C) was identified as a U.S. Marine Corps (USMC) member assigned to the Quantico Marine Corps Base. (b)(7)(C) was subsequently interviewed. He reported that only one unauthorized charge was placed on his card. The charge was for flowers via the internet. (b)(7)(C) explained that on approximately May 24, 2003 he received a message on his laptop computer via the Internet, either via email or instant messaging, linking him to an AOL site. This AOL site advertised itself as the billing center. It requested he provided his credit card number to update his customer records with AOL. (b)(7)(C) said he did so.

(b)(7)(C) also consented to a search of his computer for evidence of the reported fraud. He signed the appropriate form and returned it to the OIG. (b)(7)(C) also made available his laptop computer for imaging the next day.

On July 2, 2003 an (b)(7)(C) search was conducted on (b)(7)(C). Appropriate personal information on both individuals was obtained. The records indicate that both individuals reside at (b)(7)(C).

On July 11, 2003 OIG subpoenas were served on FTD.COM, 1-800-FLOWERS.com and Hotmail.com for records relevant to this incident. Hotmail's reply on July 14, 2003 indicated that it did not have a record identifiable with (b)(7)(C). 1-800-FLOWERS.com reply to the subpoena was received on August 1, 2003. They confirmed that a flower order was placed using the credit card number of (b)(7)(C) via the internet. The order was delivered to (b)(7)(C). The order contained a note which made threats of violence.

On August 5, 2003 online research was conducted on IP (b)(7)(C) in an effort to identify the source of the attacks using the USPS website. (b)(7)(C); (b)(7)(E)

(b)(7)(C); (b)(7)(E)
(b)(7)(C); (b)(7)(E) On August 20, 2003 a subpoena was served on the Pacific-Marine Federal Credit Union (PMFCU) for the account records of (b)(7)(C). A review of (b)(7)(C) PMFCU records indicated that a debit card as identified: Visa Check Card Classic (Debit Card) (b)(7)(C) was used to place an order on May 30, 2003. The order was placed via the internet on the ftd.com website for flowers. (b)(7)(C) subsequently contacted PMFCU on May 31, 2003 to report the fraudulent order.

On August 20, 2003 FTD.COM complied with the subpoena. A review of the FTD.com records reflected that on May 28, 2003 an Internet purchase of flowers was placed using (b)(7)(C). The flowers were sent to (b)(7)(C) with another threatening note. On September 30, 2003 an interview of (b)(7)(C) Corporate Counsel for 1-800-FLOWERS.com, disclosed that there were no additional computer records available to identify the source of the fraudulent Internet transaction on May 29, 2003.

A computer forensics exam of (b)(7)(C) computer completed on November 29, 2003 developed no additional investigative leads into the fraudulent Internet activity.

IV. LAW ENFORCEMENT AND OTHER RECORDS

A review of law enforcement records disclosed no criminal records for (b)(7)(C).
(b)(7)(C) An interview of (b)(7)(C) disclosed that (b)(7)(C) was
suspected of committing (b)(7)(C) in the (b)(7)(C) area of jurisdiction. (b)(7)(C) also
disclosed that (b)(7)(C) had a history of (b)(7)(C).

V. JUDICIAL/ADMINISTRATIVE REFERRALS

None.

VI. STATUTES

This investigation was conducted under suspected violations of 18 USC 1343 (Wire Fraud) and 18 USC 1029 (Fraud using an access device).

VII. SUBJECTS

(b)(7)(C)
Social Security Number: (b)(7)(C)
DOB:
Home Address:
Phone(s):

(b)(7)(C)
Social Security Number: (b)(7)(C)
DOB:
Home Address:
Home Phone:
Other Phone(s):

VIII. DISPOSITION OF EVIDENCE, CONTRABAND, AND PROPERTY

N/A

IX. STATUS OF INVESTIGATION

This investigation is closed because of no additional investigative leads and a lack of evidence.

X. EXHIBITS

- 1) USpscirt Incident Report, 020502-00
- 2) AR: Email to (b)(7)(C) June 10, 2002
- 3) AR: Interview of (b)(7)(C) June 13, 2002
- 4) AR: Subpoena to AT&T, June 21, 2002
- 5) AR: Subpoena to Hotline, June 19, 2002
- 6) AR: (b)(7)(C); (b)(7)(E) December 19, 2002
- 7) AR: Interview of C-001, January 14, 2003
- 8) AR: Interview of (b)(7)(C) January 14, 2003
- 9) AR: Interview of C-001, January 15, 2003
- 10) AR: Interview of (b)(7)(C) January 15, 2003
- 11) AR: Interview of (b)(7)(C) January 22, 2003
- 12) AR: Mail Cover Request, January 27, 2003
- 13) AR: Interview of (b)(7)(C) February 4, 2003
- 14) AR: Interview of (b)(7)(C) May 30, 2003
- 15) AR: Interview of (b)(7)(C) June 2, 2003
- 16) AR: Interview of (b)(7)(C) June 19, 2003
- 17) AR: Interview of (b)(7)(C) June 19, 2003
- 18) AR: Consent to Search, June 19, 2003
- 19) AR: Obtaining the laptop computer, June 19, 2003
- 20) AR: Return of the laptop computer, June 20, 2003
- 21) AR: (b)(7)(C); (b)(7)(E) July 2, 2003
- 22) AR: (b)(7)(C); (b)(7)(E) July 2, 2003
- 23) AR: Subpoena service on FTD.COM, July 11, 2003
- 24) AR: Subpoena service on 1-800-FLOWERS.com, July 11, 2003
- 25) AR: Subpoena service on Hotmail.com, July 11, 2003
- 26) AR: Subpoena reply from Hotmail.com, July 14, 2003

Page 7

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

- 27) AR: Subpoena reply from 1-800-FLOWERS.com, July 11, 2003
- 28) AR: (b)(7)(C); (b)(7)(E) August 5, 2003
- 29) AR: Subpoena service on PMFCU, August 20, 2003
- 30) AR: Subpoena reply from FTD.COM, August 20, 2003
- 31) AR: Subpoena reply from PMFCU, September 2, 2003
- 32) AR: Records review of PMFCU, September 2, 2003
- 33) AR: Interview of (b)(7)(C) September 30, 2003
- 34) Computer Forensics Exam, November 29, 2003



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
1735 NORTH LYNN STREET
ARLINGTON, VA 22209-2020

DATE: October 30, 2003

PREPARED BY: (b)(7)(C)

CASE #: 02UIHQ0639S3CT

CROSS REFERENCE #:

TITLE: UNAUTHORIZED POSSESSION OF USPS COMPUTER USERNAME IDENTIFICATIONS AND PASSWORDS

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM July 2002 TO November 2003

LOCATION OF OFFENSE: North Metro P&DC, Duluth, GA

STATUS OF CASE: Closed

- ☐ CONTINUING INVESTIGATION
- ☐ SIGNIFICANT DEVELOPMENT
- ☐ PROSECUTION REPORT
- ☐ PENDING JUDICIAL ACTION
- ☐ PENDING ADMINISTRATIVE ACTION
- ☐ PENDING OTHER ACTION
- ☐ REFERRAL TO ANOTHER AGENCY
- ☒ CLOSED

JOINT AGENCIES:

DISTRIBUTION:

TABLE OF CONTENTS

INTRODUCTION

This investigation was initiated upon receipt of information that an unknown employee of the U.S. Postal Service (Postal) was in unauthorized possession of passwords and account names of other Postal employees. This activity is in direct violation of Postal manual AS-805 and 18 USC 1030.

SYNOPSIS

This investigation concerned an allegation that a Postal employee, (b)(7)(C) had compromised Postal computer network security by obtaining account names and passwords and then using this information to send email with a religious theme to coworkers. A note was found in or near the area where (b)(7)(C) worked with other Postal employees. The note contained the account names and passwords. (b)(7)(C) denied owning or possessing any note with account names and passwords. Postal employees did not know where the note came from or how it appeared in (b)(7)(C) work area. No evidence or testimony was developed to implicate (b)(7)(C) or any other Postal employee in any wrongdoing.

NARRATIVE

On July 11, 2002, (b)(7)(C) Postal, provided a document containing logon identifications and passwords. (b)(7)(C) said (b)(7)(C) Maintenance Operations Support Department, provided him the document in approximately June 2002. (b)(7)(C) informed him that the document was discovered on a desk utilized by a Maintenance Operations Support Department employee, (b)(7)(C)

On 17 July 2002, (b)(7)(C) Information Systems, Atlanta District Office reported that a Postal employee was in unauthorized possession of passwords of other Postal employees. (b)(7)(C) identified this employee as (b)(7)(C) a Maintenance Support employee at the South Atlanta P&DC. He said that post-it note was found with account names and passwords.

On July 17, 2002, (b)(7)(C) Postal, was interviewed regarding (b)(7)(C) discovery that (b)(7)(C) account was used to send unauthorized email. (b)(7)(C); (b)(3); Pub. L. No. 95-452 62 Stat. 1101

(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

On July 17, 2002, (b)(7)(C) Postal, was interviewed regarding the possible compromise of (b)(7)(C) Postal computer account. (b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

On July 17, 2002 (b)(7)(C) Postal, was interviewed regarding the possible compromise of (b)(7)(C) Postal computer account. (b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

On July 17, 2002, (b)(7)(C) Postal, was interviewed regarding the discovery of a post-it note containing Postal account names and passwords. (b)(7)(C), (b)(3): Pub. L. No. 95-452 92

(b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

On July 17, 2002, (b)(7)(C) Postal, was interviewed regarding the possible compromise of Postal computer accounts and passwords. (b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101

On July 18, 2002 Special Assistant U.S. Attorney (SAUSA), (b)(7)(C) U.S. Attorneys Office, Northern District of Georgia, was briefed on the facts of the investigation to date. (b)(7)(C) expressed interest in this investigation.

On August 22, 2002, a network monitoring computer was placed on the network of the North Metro P&DC for the purpose of capturing network traffic from (b)(7)(C) computer.

On February 4, 2003, (b)(7)(C), (b)(7)(E)

(b)(7)(C), (b)(7)(E)

(b)(7)(C); (b)(7)(E)

On February 7, 2003, a review of computer logs obtained from (b)(7)(C); (b)(7)(E) established on the Postal network at the North Metro P&DC was reviewed. The logs contained no evidence of inappropriate network activity by (b)(7)(C).

On March 12, 2003, a drive-by of the residence at (b)(7)(C) was conducted. The residence is owned by (b)(7)(C) a Postal employee. The purpose of the drive-by was to identify any automobiles, motorcycles in or around the property. The residence is a single family home with an attached garage. No evidence of an automobile or motorcycle could be seen near or around the property.

On March 13, 2003, (b)(7)(C) Postal, was interviewed to obtain background information regarding the maintenance operations support (MOS) team and (b)(7)(C) role on the team. The MOS is responsible for maintaining and managing stock inventory for the mail processing equipment (MPE) at the P&DC. This includes inventory maintenance and ordering, hardware assignments, and software updates. (b)(7)(C) explained that (b)(7)(C) can and does take part in all of these assignments as needed. Regarding the note recovered in June 2002 with user names and passwords, she was asked if (b)(7)(C) needed the account names and passwords of other users on the MOS, she said no. Each user including (b)(7)(C) according to (b)(7)(C) has a sufficient level of access to the computer to conduct their jobs.

On March 13, 2003, (b)(7)(C) North Metro P&DC, Postal, was interviewed concerning an allegation that (b)(7)(C) illicitly obtained account names and passwords of coworkers. (b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101

On November 12, 2003, (b)(7)(C) was reinterviewed regarding this investigation. (b)(7)(C) reports no further incidents involving notes containing passwords/accounts, inappropriate emails, or other unauthorized uses of Postal computer equipment and networks.

LAW ENFORCEMENT AND OTHER RECORDS

On February 4, 2003, (b)(7)(C); (b)(7)(E)

(b)(7)(C); (b)(7)(E)

JUDICIAL/ADMINISTRATIVE REFERRALS

This matter was referred to the U.S. Attorney's Office for the Northern District of Georgia. This case was declined because of the lack of evidence.

JUDICIAL/ADMINISTRATIVE ACTION

None required. No administrative action was requested.

SUBJECTS

Name:

(b)(7)(C)

SSN:

DOB:

DISPOSITION OF EVIDENCE, CONTRABAND, AND PROPERTY

All evidence is currently in the evidence facility at the OIG office in Raleigh, NC.

STATUS OF INVESTIGATION

Closed.

EXHIBITS

- (1) Interview of (b)(7)(C); July 11, 2002
- (2) Interview of (b)(7)(C); July 17, 2002
- (3) Interview of (b)(7)(C); July 17, 2002
- (4) Interview of (b)(7)(C); July 17, 2002
- (5) Interview of (b)(7)(C); July 17, 2002
- (6) Interview of (b)(7)(C); July 17, 2002
- (7) Interview of (b)(7)(C); July 17, 2002

- (8) Meeting with (b)(7)(C); July 18, 2002
- (9) Installation of Network Monitor/August 22, 2002
- (10) (b)(7)(C); (b)(7)(E) February 4, 2003
- (11) Review of Network (b)(7)(C); Logs/February 7, 2003
- (12) Drive-By of Residence/March 12, 2003
- (13) Interview of (b)(7)(C); March 13, 2003
- (14) Interview of (b)(7)(C); March 13, 2003
- (15) Interview of (b)(7)(C); November 12, 2003

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
11698 NW 25th STREET
MIAMI, FL 33112

CASE #: 05UIMI4153S3IO

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM May 5, 2005 TO July 7, 2005

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES:

N/A

DISTRIBUTION:

N/A

PREPARED BY: SA (b)(7)(C)	DATE: 7/7/2005
APPROVED BY: BOLTE, DONALD	DATE: 7/13/2005

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

TABLE OF CONTENTS

- I. PREDICATION
- II. POTENTIAL VIOLATIONS
- III. SYNOPSIS
- IV. BACKGROUND
- V. DETAILS
- VI. DISPOSITION
- VII. EXHIBITS

I. PREDICATION

This investigation was based on a hotline complaint filed by (b)(7)(C) Human Resource Specialist (HRS), United States Postal Service (USPS) and (b)(7)(C) Acting HRS, USPS, alleging a conflict of interest by (b)(7)(C) (b)(7)(C) Post Office, USPS.

(b)(7)(C) has allegedly been directing USPS employees at the (b)(7)(C) Post Office to buy insurance from (b)(7)(C) insurance salesman, just off USPS property as they return from their routes. (b)(7)(C) allegedly encourages the USPS employee to purchase insurance from this salesman stating that he has purchased insurance from him, and that the salesman is "legit".

(b)(7)(C) had allegedly convinced USPS employees to compromise the security of PostalEase by giving their passwords and pin numbers to him through his sales pitch.

II. POTENTIAL VIOLATIONS

An investigation is required in order to develop evidence leading to possible criminal and/or civil prosecution under Title 18 USC 641 (Public money, property or records) Title 18 USC 1030 (Fraud Related to the Connection of Computers) , Title 18 USC 1343 (Fraud by Wire Telephone or Television), or other civil/administrative proceeding as appropriate.

III. SYNOPSIS

The investigation determined that there was no evidence to support the allegation that (b)(7)(C) convinced USPS employees to compromise the security of PostalEase by giving him their pin numbers. There was no evidence to support the allegation that (b)(7)(C) directed employee's to (b)(7)(C). However, there was some evidence to support the fact that (b)(7)(C) encouraged employee's to purchase insurance from (b)(7)(C).

(b)(7)(C), (b)(7)(E)

(b)(7)(C) stated that he taped (b)(7)(C) sales meeting notice to the employee time clock, and he made an announcement that (b)(7)(C) would be outside. (b)(7)(C) stated that he did inform USPS employee's about (b)(7)(C) services, and that he had purchased insurance from (b)(7)(C) in 1990/91.

(b)(7)(C) USPS, stated that (b)(7)(C) told him and other employees on USPS property that (b)(7)(C) was located just outside the gate, and would provide a free financial analysis of their projected retirement. (b)(7)(C) said that (b)(7)(C) posted a notice of the free financial planning on the time clock, so he thought that the USPS had endorsed (b)(7)(C)

IV. BACKGROUND

This investigation was based on a hotline complaint filed by (b)(7)(C) alleging a conflict of interest by (b)(7)(C). On May 5, 2005 the allegation was assigned to the RA.

V. SUPPORTING DETAILS

On May 6, 2005 the RA talked with (b)(7)(C) regarding the allegation they submitted on May 5, 2005. (b)(7)(C) stated that on May 4, 2005 she was contacted by (b)(7)(C) USPS, regarding an experience (b)(7)(C) had with (b)(7)(C) Insurance Salesman. (b)(7)(C) stated that after she was contacted she notified (b)(7)(C) who contacted (b)(7)(C) HR Manager, and upon approval of (b)(7)(C) the allegation was submitted to the Office of Inspector General. Neither (b)(7)(C) had any direct knowledge of the allegation. (b)(7)(C) provided the RA with a signed copy of a statement she made regarding information she received from (b)(7)(C) during a telephone conversation on May 4, 2005.

On May 5, 2005, the RA interviewed (b)(7)(C) provided the following information. (b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3); Pub. L. No. 95-452 92 Stat. 1101



On May 5, 2005, the RA interviewed (b)(7)(C), (b)(3); Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3); Pub. L. No. 95-452 92 Stat. 1101



On May 5, 2005, at 5:00PM the reporting agent (RA) (b)(7)(C), (b)(7)(E)

(b)(7)(C), (b)(7)(E)



(b)(7)(C); (b)(7)(E)



VI. DISPOSITION

There was no evidence to support the allegation, so this investigation is closed.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
P. O. BOX 430187
BIRMINGHAM, AL 35243-1187

CASE #: 07UIBH0777CI3MS

CROSS REFERENCE #:

TITLE: (b)(7)(C)
MISUSE OF USPS COMPUTER VFO
CALL 061018VFO015

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM October 18, 2006 **TO** June 5, 2007

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES:

None

DISTRIBUTION:

Closed Case File

PREPARED BY: SA (b)(7)(C)	DATE: 06/05/07
APPROVED BY: ASAC L Norrington	DATE:

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

I. PREDICATION

On October 18, 2006, the United States Postal Service (USPS) Office of Inspector General (OIG), received an allegation from (b)(7)(C) (b)(7)(C) Huntsville, AL, USPS. (b)(7)(C) alleges that on September 14, 2006, (b)(7)(C) Arab Post Office, USPS, Arab, AL used her USPS computer to fraudulently open an account with Cingular Wireless using his social security number. Cingular Wireless alerted (b)(7)(C) to the fraudulent account access using USPS access.

II. SYNOPSIS

A computer search was conducted by the OIG to identify Web log activities of the postal service computer access of (b)(7)(C) computer usage on September 14, 2006. The search revealed numerous accesses of the Cingular Wireless web site on the morning of September 14, 2006. (b)(7)(C) was interviewed on March 1, 2007. (b)(7)(C) did not confirm or deny the illegal access to (b)(7)(C) cell phone account but did state she was sorry and it would not happen again.

III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

On October 18, 2006, the OIG opened an investigation into an allegation received from (b)(7)(C) (b)(7)(C) alleges that on September 14, 2006, (b)(7)(C) (b)(7)(C) used her USPS computer to fraudulently open an account with Cingular Wireless using his social security number. Cingular Wireless alerted (b)(7)(C) (b)(7)(C) to the fraudulent account access using USPS access.

A computer search was requested to identify Web log activities of the postal service computer access of (b)(7)(C) computer usage on September 14, 2006. The search revealed (b)(7)(C) was on numerous Cingular web sites from 5:15am to 6:38am on September 14, 2006 (Exhibit 1).

On March 1, 2007, RA interviewed (b)(7)(C) (b)(7)(C) Postmaster, Arab Post Office, USPS, Arab, AL 35016 witnessed the interview. The interview was in

reference to an allegation concerning (b)(7)(C) fraudulently accessing (b)(7)(C) cell phone account while using a USPS computer.

(b)(7)(C), (b)(3): Pub. L. No. 95-452 92 Stat. 1101



V. DISPOSITION

On March 27, 2007 (b)(7)(C) received an official discussion.

VI. EXHIBITS

1. Copy of a Web Log activity report of (b)(7)(C) postal service computer access on September 14, 2006.
2. Copy of an OIG Acknowledgement of Rights form dated March 1, 2007 and signed by (b)(7)(C), (b)(3): Pub. L.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
8400 NW 36th St, Suite 260
MIAMI, FL 33166

Date: March 19, 2007

(b)(7)(C)

Postmaster
819 N Main St.
Arab, AL 35016

Subject: (b)(7)(C)

Reference: OIG Case No. 07UIBH0777CI3MS

RESTRICTED INFORMATION

The U.S. Postal Service, Office of Inspector General (OIG) recently conducted an investigation on (b)(7)(C) Arab Post Office, United States Postal Service (USPS), Arab AL 35016. Investigation has disclosed (b)(7)(C) misused her USPS computer to fraudulently accessing (b)(7)(C) cell phone account. The attached Report of Investigation and exhibits are submitted for your consideration and decision as to whether disciplinary action is warranted.

Please advise me, in writing within 30 days, of your decision in this matter. If you decide to take disciplinary action, please furnish me a copy of the letter to the employee and your final decision letter.

The Report of Investigation is "Restricted Information." All OIG reports are furnished on an official need to know basis and must be protected from dissemination that may compromise the best interest of the U.S. Postal Service.

If you have any questions or need additional information, please contact Special Agent

(b)(6), (b)(7)(C)

James Davis
Special Agent-In-Charge
Miami Field Office

Enclosure: Report of Investigation



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

P. O. BOX 430187
BIRMINGHAM, AL 35243-1187

CASE #: 07UIBH0777CI3MS

CROSS REFERENCE #:

TITLE: (b)(7)(C)
**MISUSE OF USPS COMPUTER VFO
CALL 061018VFO015**

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM October 18, 2006 **TO** March 1, 2007

STATUS OF CASE: CLOSED PENDING (ADMINISTRATIVE)

JOINT AGENCIES:

None

DISTRIBUTION:

(b)(7)(C)
Postmaster
819 N Main St.
Arab, AL 35016

PREPARED BY: SA (b)(7)(C)	DATE: 3/06/07
APPROVED BY: ASAC Nick Ivanovic	DATE: 3/06/07

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

I. PREDICATION

On October 18, 2006, the United States Postal Service (USPS) Office of Inspector General (OIG), received an allegation from (b)(7)(C) (b)(7)(C) Huntsville, AL, USPS. (b)(7)(C) alleges that on September 14, 2006, (b)(7)(C) Arab Post Office, USPS, Arab, AL used her USPS computer to fraudulently open an account with Cingular Wireless using his social security number. Cingular Wireless alerted (b)(7)(C) to the fraudulent account access using USPS access.

II. SYNOPSIS

A computer search was conducted by the OIG to identify Web log activities of the postal service computer access of (b)(7)(C) computer usage on September 14, 2006. The search revealed numerous accesses of the Cingular Wireless web site on the morning of September 14, 2006. (b)(7)(C) was interviewed on March 1, 2007. (b)(7)(C) did not confirm or deny the illegal access to (b)(7)(C) cell phone account but did state she was sorry and it would not happen again.

III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

On October 18, 2006, the OIG opened an investigation into an allegation received from (b)(7)(C) (b)(7)(C) alleges that on September 14, 2006, (b)(7)(C) (b)(7)(C) used her USPS computer to fraudulently open an account with Cingular Wireless using his social security number. Cingular Wireless alerted (b)(7)(C) (b)(7)(C) to the fraudulent account access using USPS access.

A computer search was requested to identify Web log activities of the postal service computer access of (b)(7)(C) computer usage on September 14, 2006. The search revealed (b)(7)(C) was on numerous Cingular web sites from 5:15am to 6:38am on September 14, 2006 (Exhibit 1).

On March 1, 2007, RA interviewed (b)(7)(C) Postmaster, Arab Post Office, USPS, Arab, AL 35016 witnessed the interview. The interview was in

V. DISPOSITION

All investigative issues have been concluded. This investigation is being referred to postal management in support of whatever action deemed appropriate.

VI. EXHIBITS

1. Copy of a Web Log activity report of (b)(7)(C) postal service computer access on September 14, 2006.
2. Copy of an OIG Acknowledgement of Rights form dated March 1, 2007 and signed by (b)(7)(C).
(b)(3): Pub. L. No.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

MARQUIS 1, SUITE 2000
245 PEACHTREE CENTER AVE, NE
ATLANTA, GA 30303

CASE #: 07UIGR4325CI3MS

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

SHORT-FORM REPORT OF INVESTIGATION

PERIOD COVERED: FROM March 3, 2007 TO June 25, 2007

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES:

DISTRIBUTION:

PREPARED BY: (b)(7)(C)

DATE: 6/25/07

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

PREDICATION: On March 3, 2007, the Greensboro, North Carolina Police Department arrested (b)(7)(C) an employee at the Human Resources Shared Services Center (HRSSC) in Greensboro on charges related to a major bank fraud scheme. A search of (b)(7)(C) apartment revealed documents containing the personal identification information of several individuals.

The focus of this investigation was to determine if (b)(7)(C) used electronic access to the Postal Service's personnel records to commit identity theft.

DETAILS:

Allegation 1 (b)(7)(C) used Postal Service data systems at the HRSSC to obtain personal identification information of Postal Service employees in furtherance of an identity theft operation.

Allegation 1 Findings No evidence was found to show (b)(7)(C) stole personal identification information accessed through (b)(7) employment with the Postal Service. On March 28, 2007, the HRSSC provided the names of individuals whose files were assigned to (b)(7)(C)

The hard drive from (b)(7)(C) computer was imaged and searched by the Computer Crimes Unit. The CCU did not find evidence of (b)(7)(C) improperly accessing employee data, of any internet use, or (b)(7)(C) using email to send personal identification data via email. The names found in the data on the drive have been documented in the event of future incidents of identity theft involving these individuals.

On May 30, 2007, Greensboro, North Carolina Police Department Detective (b)(7)(C) advised that the personal identification information found at (b)(7)(C) apartment appears to have originated at North Carolina A&T University, (b)(7)(C)

DISPOSITION: The investigation did not reveal evidence that (b)(7)(C) used (b)(7)(C) access to Postal Service data to commit identity theft. This case is closed.

EXHIBITS: None.

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

433 WEST HARRISON
SUITE 4000
CHICAGO, IL 60699-4000

CASE #: 08UICH4504GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

(b)(7)(C) **POST OFFICE)**

CASE AGENT (if different from prepared by):

CASE SUMMARY REPORT

PERIOD COVERED: FROM April 15, 2008 **TO** June 18, 2008

STATUS OF CASE: CLOSED INVESTIGATION UNFOUNDED

SUMMARY OF INVESTIGATIVE ACTIVITY:

On April 15, 2008, the United States Postal Service (USPS) Office of Inspector General (OIG) received a complaint from (b)(7)(C) suspects a USPS employee, (b)(7)(C) Post Office, of obtaining her Discover Card number and using it to purchase a \$1400 Dell computer via the internet.

SA (b)(7)(C) queried USPS databases, specifically the Retail Data Mart (RDM) and obtained the exact time, 11:35 am, that (b)(7)(C) assisted (b)(7)(C) with her transactions. SA (b)(7)(C) contacted Dell investigators and requested the date, time and Internet Protocol Address (IP) of the individual that logged onto the Dell website to purchase a Dell computer using the credit card information from (b)(7)(C). Dell investigators provided an IP address of (b)(7)(C) on March 28, 2008 at 11:22 am.

SA (b)(7)(C) served an IG subpoena on Comcast Internet Services for the above listed IP address. The information received did not match that of (b)(7)(C). In addition, (b)(7)(C) waited on (b)(7)(C) 13 minutes after (b)(7)(C) credit card information was already used.

The following is the information obtained from Comcast Internet Services:

Subscribers name: (b)(7)(C)

Address:

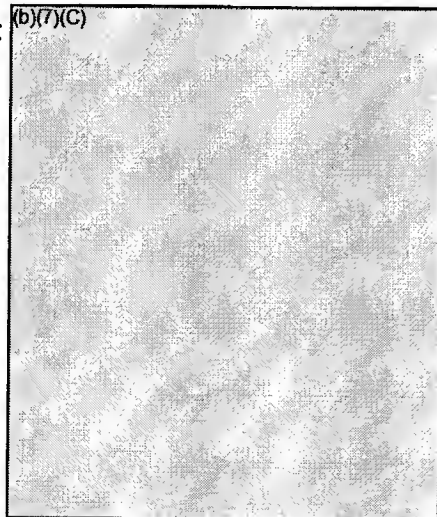
Telephone:

Account Status:

Account Created:

Account Number:

Email User ID:



This information was passed on to Dell investigators. In addition, (b)(7)(C) was notified that (b)(7)(C) was not involved in the capturing of her credit card information.

This case is closed, no further action is necessary.

PREPARED BY: SA (b)(7)(C)	DATE: 6-18-08
APPROVED BY: ASAC John Farrell	DATE: 6-18-08



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL
433 WEST HARRISON
SUITE 4000
CHICAGO, IL 60699-4000**

CASE #: 08UIIN7062GC04GC **CROSS REFERENCE #:**
TITLE: MISUSE OF CHANGE OF
ADDRESS FORWARDING SYSTEM,
INDIANAPOLIS, IN 46201
CASE AGENT (if different from prepared by):

CASE SUMMARY REPORT

PERIOD COVERED: FROM AUGUST 21, 2008 TO August 28, 2008

STATUS OF CASE: CLOSED INVESTIGATION UNFOUNDED

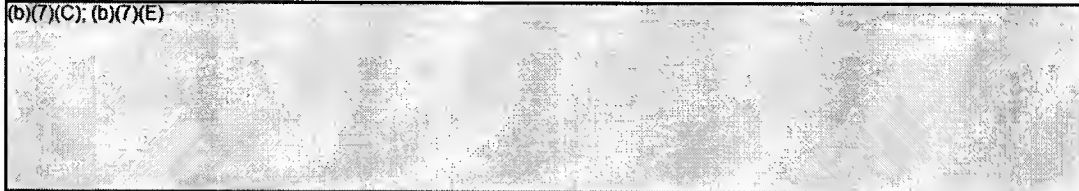
SUMMARY OF INVESTIGATIVE ACTIVITY:

On August 13, 2008, unknown suspects using an email address of (b)(7)(C) submitted a false change of address via the U.S. Postal Service Change of Address Forwarding System for postal customer (b)(7)(C) IN 46164 to (b)(7)(C) IN 46201. Internet Protocol (IP) address (b)(7)(C) was captured during the transaction. (b)(7)(C) was the victim of a residential burglary where her personal information was also stolen.

(b)(7)(C) U. S. Postal Inspector has requested assistance in obtaining information from the Service Provider for the IP address and the e-mail account holder.

PREPARED BY: SA (b)(7)(C)	DATE: 8/28/2008
----------------------------------	------------------------

On August 21, 2008, a case was opened and three subpoenas were requested through E-Subpoena. The Office of General Counsel (OGC) questioned the investigative jurisdiction of the Office of Inspector General (OIG) in the investigation. Special Agent (b)(7)(C) informed (b)(7)(C) Senior Attorney, OGC, that the reason the case was opened was to assist the Inspection Service in obtaining the subpoena information. (b)(7)(C) directed SA (b)(7)(C) to OIG Investigative Manual section 304.2.4 paragraph 5.



On August 28, 2008, SA (b)(7)(C) contacted the investigating Inspector regarding the closure of the case. No further action is warranted in this case. This case is to be closed.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

PO BOX 454
JERSEY CITY, NJ 07303

CASE #: 08UINY3819GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

**FRAUDULENT CREDIT
APPLICATION**

CASE AGENT (if different from prepared by):

CASE SUMMARY REPORT

PERIOD COVERED: FROM: March 13, 2008 **TO:** April 8, 2008

STATUS OF CASE: CLOSED INVESTIGATION

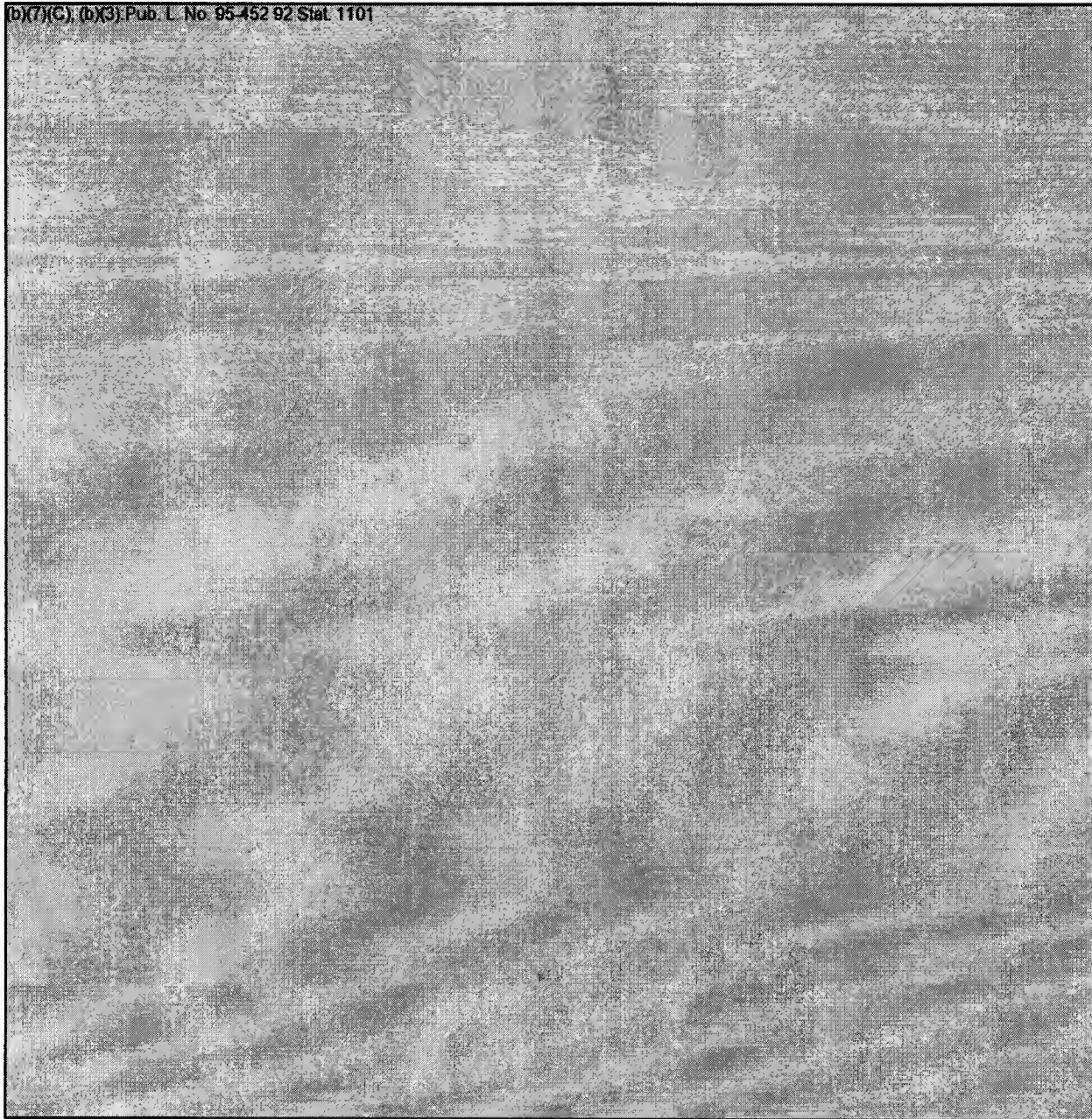
SUMMARY OF INVESTIGATIVE ACTIVITY:

The United States Postal Service Office of Inspector General's New York Area Field Office received information that (b)(7)(C) appears to have submitted a fraudulent credit application to Commerce Bank on January 25, 2008.

The credit application submitted was under the name of (b)(7)(C). A check of Postal databases show that (b)(7)(C) is not a Postal employee. Commerce Bank contacted (b)(7)(C) at her residence in South Carolina. (b)(7)(C) stated that she did not submit the application. A review of the application showed that an additional credit card was requested for (b)(7)(C).

On March 25, 2008, USPSOIG Special Agents interviewed (b)(7)(C), (b)(3). Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3). Pub. L. No. 95-452 92 Stat. 1101



RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

Information about (b)(7)(C) will be shared with the United States Postal Inspection Service. Due to any further investigative leads relating to any Postal employees, this case is being closed.

ATTACHMENT 1

(b)(7)(C) MOI 032508

PREPARED BY: SA (b)(7)(C)	DATE: 04-08-08
----------------------------------	-----------------------



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
1735 NORTH LYNN STREET
SUITE 10000
ARLINGTON, VA 22209-2020

CASE #: 08UIRF3733GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM March 4, 2008 TO April 18, 2008

STATUS OF CASE: CLOSED PENDING (JUDICIAL)

JOINT AGENCIES:

Fairfax County Police Department

DISTRIBUTION:

Case File

PREPARED BY: SA (b)(7)(C)

DATE: 4/18/08

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

I. PREDICATION

On Wednesday, February 27, 2008, the United States Postal Service (USPS), Office of Inspector General (OIG), Capital Metro Area Field Office received an investigative referral from the Fairfax County, VA, Police Department regarding (b)(7)(C) contract employee for Manpower Inc (Manpower), USPS Merrifield Engineering Department. Fairfax County police arrested (b)(7)(C) February 14, 2008, for multiple felonies involving a burglary and stolen credit cards and other items. A further criminal history check for (b)(7)(C) is positive for previous arrests for one felony and one misdemeanor (Exhibit 1)

II. SYNOPSIS

(b)(7)(C) was arrested and charged with three felonies while employed with Manpower and assigned to the USPS Engineering Department in Merrifield, VA. (b)(7)(C) failed to disclose her arrest to Manpower and the USPS. When the OIG notified USPS management of (b)(7)(C) arrest, she was immediately escorted from the Engineering building and Manpower subsequently removed her from the USPS contract. However, Manpower continues to employ (b)(7)(C) and the company has not taken any steps to terminating her employment as of the date of this report.

III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

Allegation 1: (b)(7)(C) was arrested for off-duty criminal misconduct and failed to disclose this information to (b)(7)(C) or the USPS.

On March 7, 2008, Special Agent (SA) (b)(7)(C) contacted Detective (b)(7)(C) Fairfax County Police Department, West Springfield Station. Detective (b)(7)(C) is currently investigating the burglary and associated thefts involving several individuals, including (b)(7)(C) said (b)(7)(C) was arrested on February 14, 2008, on three felony larceny charges stemming from a burglary on (b)(7)(C) is accused of using personal credit cards that were stolen from a Fairfax residence on

that day. (b)(7)(C) was arrested with (b)(7)(C) who is still in jail facing additional charges. (b)(7)(C) said (b)(7)(C) posted a \$3,000 bond and is due in court for her preliminary hearing in May 2008 (Exhibits 2).

An OIG review of publicly available court records indicated that (b)(7)(C) was charged with three felonies on February 14, 2008. Two of the charges are for credit card fraud and the third relates to receiving stolen property (Exhibits 3-5).

On March 7, 2008, SA (b)(7)(C) met with (b)(7)(C) Vice President, Engineering, Merrifield, VA, regarding (b)(7)(C). SA (b)(7)(C) advised (b)(7)(C) that Fairfax County Police are currently investigating a burglary and associated thefts involving several individuals, including (b)(7)(C). SA (b)(7)(C) provided (b)(7)(C) with a copy of publicly available court records regarding (b)(7)(C) recent arrest. SA (b)(7)(C) advised (b)(7)(C) that a detective from Fairfax County had interviewed (b)(7)(C) USPS supervisor, (b)(7)(C) a day earlier regarding (b)(7)(C) work status. (b)(7)(C) said he was unaware of this. He then called his Director of Security, (b)(7)(C) as well as (b)(7)(C) to his office.

(b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat 1101



(b)(7)(C) said she would pull phone records for Thompson's USPS desk phone, (b)(7)(C) said (b)(7)(C) did not have a USPS cell phone, only a personal cell phone. (b)(7)(C) said the Manpower contract was set to expire in one month.

At the request of (b)(7)(C) escorted (b)(7)(C) from the building and seized her USPS identification badge at approximately 3:45PM. (b)(7)(C) said (b)(7)(C) gathered several personal items prior to leaving. SA (b)(7)(C) seized the two computers (b)(7)(C) routinely accessed, as well as several post-it notes containing personal identifying information and telephone numbers that (b)(7)(C) had abandoned. SA (b)(7)(C) provided these computers to the OIG's Computer Crimes Unit for analysis (Exhibit 6, 7).

Following the OIG's notification to USPS management of (b)(7)(C) pending criminal charges, SA (b)(7)(C) obtained (b)(7)(C) USPS telephone logs, internet browser history logs and e-mail archives. SA (b)(7)(C) also determined that (b)(7)(C) had access to two USPS credit cards; however, there was no fraud identified on these accounts. (b)(7)(C) did not have access to other credit cards or purchase accounts.

A review of the internet logs determined that (b)(7)(C) searched for a pawnshop seven days after the date of the burglary. This pawnshop is one of the pawnshops identified in the overall fraud scheme targeting (b)(7)(C). SA (b)(7)(C) provided this information to Det. (b)(7)(C) for use in his investigation and criminal case against (b)(7)(C) (Exhibit 8).

A review of (b)(7)(C) telephone logs also revealed that she had telephone conversations with a known criminal associate of (b)(7)(C) four times prior to the January burglary using her USPS work telephone. SA (b)(7)(C) provided this information to Det. (b)(7)(C) for use in his investigation and criminal case against (b)(7)(C) (Exhibit 9).

Allegation 2: (b)(7)(C) had a prior criminal arrest history of before she was hired by Manpower.

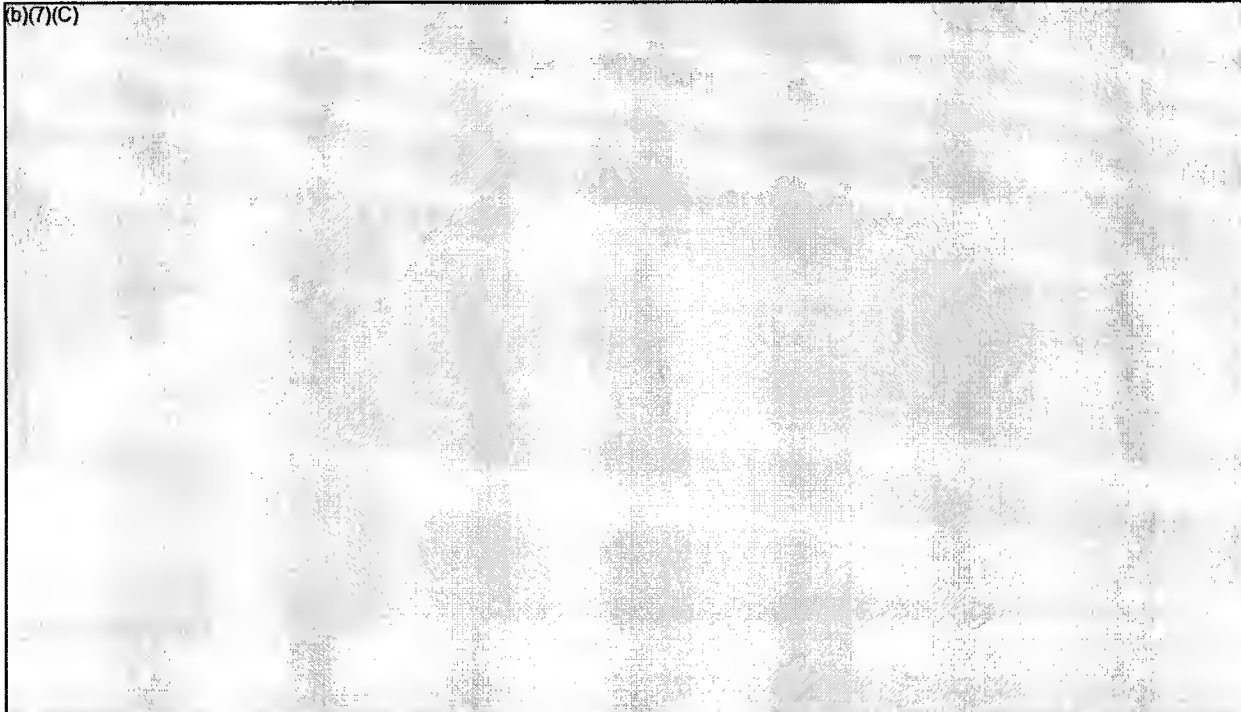
SA (b)(7)(C) reviewed a criminal history report for (b)(7)(C) which indicated she was arrested previously for felony larceny as well as for misdemeanor failing to send her child to school (truancy) (Exhibit 10).

On March 24, 2008, SA (b)(7)(C) issued an OIG Subpoena Duces Tecum to Manpower for (b)(7)(C) pre-employment, hiring and work assignment records. A review of the subpoenaed records from Manpower indicated that the USPS does not request that

contractors require employees to disclose past arrest information on their criminal history declarations. Therefore, (b)(7)(C) previous arrest history was not noted on her application to Manpower or the background forms submitted to the USPS (Exhibits 11, 12).

Allegation 3: Manpower continued to employ (b)(7)(C) after learning that she failed to disclose her arrest in February 2008, stemming from three felony theft and stolen property charges.

On March 10, 2008, SA (b)(7)(C) interviewed (b)(7)(C) Branch Manager, Manpower, Springfield, VA, regarding (b)(7)(C)



On March 28, 2008, SA (b)(7)(C) interviewed (b)(7)(C) again as a follow-up to an OIG subpoena that was issued to Manpower on March 24, 2008. (b)(7)(C) said she received the OIG subpoena for records related to (b)(7)(C) employment with Manpower. (b)(7)(C) said she engaged her Legal Affairs office to assist in preparing the OIG subpoena results. SA (b)(7)(C) asked about the status of (b)(7)(C) employment and whether Manpower had terminated (b)(7)(C) from the company. (b)(7)(C) said (b)(7)(C) is still registered with Manpower, meaning that she is still available for assignment. (b)(7)(C) declined to comment on whether Manpower has assigned (b)(7)(C) to work at another location at this time. SA (b)(7)(C) asked (b)(7)(C) why Manpower had not initiated

termination proceedings against (b)(7)(C) based on her recent arrests. (b)(7)(C) said she needed to find out who in Human Resources or Legal Affairs would be best to answer that question (Exhibit 14).

On April 9, 2008, SA (b)(7)(C) interviewed (b)(7)(C) Corporate Counsel, Manpower, Milwaukee, WI, regarding (b)(7)(C)

(b)(7)(C)

(b)(7)(C) said (b)(7)(C) was still an "associate" of Manpower, which means that she is available for assignment at other job locations. (b)(7)(C) confirmed that Manpower would not assign (b)(7)(C) to another USPS site; however, (b)(7)(C) said Manpower did not intend to fire (b)(7)(C) at this time. (b)(7)(C) said several times that (b)(7)(C) is merely charged with crimes, and that these are simply allegations. (b)(7)(C) said normally when an associate is accused of crimes involving theft or similar dishonesty, Manpower will seek work opportunities for that person at locations where it is less likely that they will have the opportunity to commit such crimes, such as product assembly work.

(b)(7)(C) said Manpower does not disclose to potential employers that the associate is currently facing criminal charges. (b)(7)(C) said in the case of (b)(7)(C) if she was assigned to another agency, Manpower is under no obligation to notify that employer of her current criminal charges. (b)(7)(C) said that even if (b)(7)(C) was convicted, she might still be able to keep working for Manpower.

(b)(7)(C) said that Manpower does not ask its associates whether they are currently facing criminal charges, only whether they have been convicted of crimes. (b)(7)(C) said in certain states, it is illegal for Manpower to ask associates whether they had ever been arrested before, assuming they were not convicted. In addition, (b)(7)(C) said certain states prohibit Manpower from disclosing that an associate is facing criminal charges.

When asked how she would characterize the removal of (b)(7)(C) from the USPS contract, (b)(7)(C) said, (b)(7)(C) access to the USPS facilities was terminated on (b)(7)(C) as far as Manpower is concerned." (b)(7)(C) said Manpower would be sure

never to reassign (b)(7)(C) to another USPS contract. As it relates to (b)(7)(C) pending criminal charges, SA (b)(7)(C) provided (b)(7)(C) with the contact information for the Fairfax County Clerk of Courts (Exhibit 15).

V. DISPOSITION

Investigative activity by the OIG has concluded and all relevant information was provided to the Fairfax County Police Department. This Report of Investigation is prepared as an investigative summary for the official case file. (b)(7)(C) is scheduled to appear at Fairfax County Circuit Court for trial in May 2008.

VI. EXHIBITS

1. Case Initiation, dated March 4, 2008.
2. Memorandum of Activity, Contact with Det. (b)(7)(C) dated March 7, 2008.
3. Felony charge 1 of 3 against (b)(7)(C)
4. Felony charge 2 of 3 against (b)(7)(C)
5. Felony charge 3 of 3 against (b)(7)(C)
6. Memorandum of Activity, OIG notification to USPS management, dated March 9, 2008.
7. Memorandum of Activity, Seizure of two USPS computers, dated March 9, 2008.
8. Forensic Lead Closure, Web Logs, dated March 10, 2008.
9. Memorandum of Activity, Analysis of USPS telephone logs, dated April 15, 2008.
10. Criminal History for (b)(7)(C)
11. OIG subpoena to Manpower, issued March 24, 2008.
12. Manpower response to OIG subpoena, dated April 7, 2008.
13. Memorandum of Interview, (b)(7)(C) dated March 10, 2008.
14. Memorandum of Interview, (b)(7)(C) dated March 28, 2008.
15. Memorandum of Interview, (b)(7)(C) dated April 9, 2008.

EMBEDDED EXHIBITS

1. Case Initiation, dated March 10, 2008.

CI - (b)(7)(C) 3-10-2008

2. Memorandum of Activity, Contact with Det. (b)(7)(C) dated March 7, 2008.

Contact with Fairfax PD - Det (b)(7)(C)

3. Felony charge 1 of 3 against (b)(7)(C)

Felony Larceny - credit cards - Fairfax County GDC

4. Felony charge 2 of 3 against (b)(7)(C)

Felony Larceny - credit cards - charge 2 - Fairfax Co GDC

5. Felony charge 3 of 3 against (b)(7)(C)

Felony Larceny - credit cards - charge 2 - Fairfax Co GDC

6. Memorandum of Activity, OIG notification to USPS management, dated March 9, 2008.

Contact with VP (b)(7)(C) arrest

7. Memorandum of Activity, Seizure of two USPS computers, dated March 9, 2008.

Seizure of two computers for (b)(7)(C)

8. Forensic lead Closure, Web Logs, dated March 10, 2008.

Forensic Lead Closure-WebLog Analysis

9. Memorandum of Activity, Analysis of USPS telephone logs, dated April 15, 2008.

Analysis of telephone logs with known associates

10. Criminal History for (b)(7)(C)

(b)(7)(C) - previous arrests noted

11. OIG subpoena to Manpower, issued March 24, 2008.

OIG subpoena to Manpower

12. Manpower response to OIG subpoena, dated April 7, 2008.

Manpower subpoena return for (b)(7)(C)

13. Memorandum of Interview, (b)(7)(C) dated March 10, 2008.

Interview of (b)(7)(C) Manpower Branch Mgr

14. Memorandum of Interview, (b)(7)(C) dated March 28, 2008.

MOI - Interview of (b)(7)(C) (2nd) 3.28.08

15. Memorandum of Interview, (b)(7)(C) dated April 9, 2008.

Interview of (b)(7)(C) Manpower Corp Counsel



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**
1735 NORTH LYNN STREET
SUITE 10000
ARLINGTON, VA 22209-2020

CASE #: 08UIRF3733GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM March 4, 2008 TO April 18, 2008

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES:

Fairfax County Police Department

DISTRIBUTION:

Case File

PREPARED BY: SA (b)(7)(C)

DATE: 7/8/08

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

I. PREDICATION

On Wednesday, February 27, 2008, the United States Postal Service (USPS), Office of Inspector General (OIG), Capital Metro Area Field Office received an investigative referral from the Fairfax County, VA, Police Department regarding (b)(7)(C) contract employee for Manpower Inc (Manpower), USPS Merrifield Engineering Department. Fairfax County police arrested (b)(7)(C) February 14, 2008, for multiple felonies involving a burglary and stolen credit cards and other items. A further criminal history check for (b)(7)(C) is positive for previous arrests for one felony and one misdemeanor (Exhibit 1)

II. SYNOPSIS

(b)(7)(C) was arrested and charged with three felonies while employed with Manpower and assigned to the USPS Engineering Department in Merrifield, VA. (b)(7)(C) failed to disclose her arrest to Manpower and the USPS. When the OIG notified USPS management of (b)(7)(C) arrest, she was immediately escorted from the Engineering building and Manpower subsequently removed her from the USPS contract. However, Manpower continues to employ (b)(7)(C) and the company has not taken any steps to terminating her employment as of the date of this report.

III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

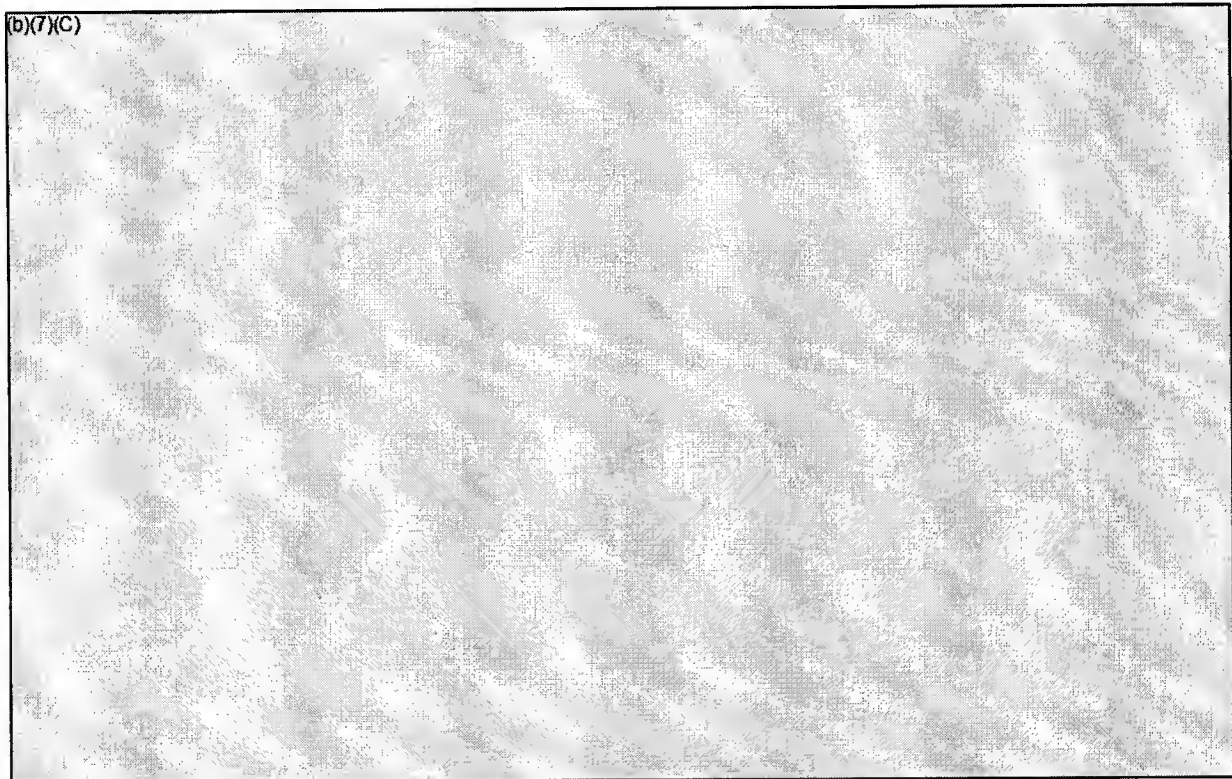
Allegation 1: (b)(7)(C) was arrested for off-duty criminal misconduct and failed to disclose this information to Manpower or the USPS.

On March 7, 2008, Special Agent (SA) (b)(7)(C) contacted Detective (b)(7)(C) Fairfax County Police Department, West Springfield Station. Detective (b)(7)(C) is currently investigating the burglary and associated thefts involving several individuals, including (b)(7)(C). (b)(7)(C) said (b)(7)(C) was arrested on February 14, 2008, on three felony larceny charges stemming from a burglary on January 3, 2008. (b)(7)(C) is accused of using personal credit cards that were stolen from a Fairfax residence on

that day. (b)(7)(C) was arrested with (b)(7)(C) who is still in jail facing additional charges. (b)(7)(C) said (b)(7)(C) posted a \$3,000 bond and is due in court for her preliminary hearing in May 2008 (Exhibits 2).

An OIG review of publicly available court records indicated that (b)(7)(C) was charged with three felonies on February 14, 2008. Two of the charges are for credit card fraud and the third relates to receiving stolen property (Exhibits 3-5).

On March 7, 2008, SA (b)(7)(C) met with (b)(7)(C) Vice President, Engineering, Merrifield, VA, regarding (b)(7)(C) SA (b)(7)(C) advised (b)(7)(C) that Fairfax County Police are currently investigating a burglary and associated thefts involving several individuals, including (b)(7)(C) SA (b)(7)(C) provided (b)(7)(C) with a copy of publicly available court records regarding (b)(7)(C) recent arrest. SA (b)(7)(C) advised (b)(7)(C) that a detective from Fairfax County had interviewed (b)(7)(C) USPS supervisor, (b)(7)(C) a day earlier regarding (b)(7)(C) work status. (b)(7)(C) said he was unaware of this. He then called his Director of Security, (b)(7)(C) as well as (b)(7)(C) to his office.



(b)(7)(C) said she would pull phone records for (b)(7)(C) USPS desk phone, (b)(7)(C) said (b)(7)(C) did not have a USPS cell phone, only a personal cell phone. (b)(7)(C) said the Manpower contract was set to expire in one month.

At the request of (b)(7)(C) escorted (b)(7)(C) from the building and seized her USPS identification badge at approximately 3:45PM. (b)(7)(C) said (b)(7)(C) gathered several personal items prior to leaving. SA (b)(7)(C) seized the two computers (b)(7)(C) routinely accessed, as well as several post-it notes containing personal identifying information and telephone numbers that (b)(7)(C) had abandoned. SA (b)(7)(C) provided these computers to the OIG's Computer Crimes Unit for analysis (Exhibit 6, 7).

Following the OIG's notification to USPS management of (b)(7)(C) pending criminal charges, SA (b)(7)(C) obtained (b)(7)(C) USPS telephone logs, internet browser history logs and e-mail archives. SA (b)(7)(C) also determined that (b)(7)(C) had access to two USPS credit cards; however, there was no fraud identified on these accounts. (b)(7)(C) did not have access to other credit cards or purchase accounts.

A review of the internet logs determined that (b)(7)(C) searched for a pawnshop seven days after the date of the burglary. This pawnshop is one of the pawnshops identified in the overall fraud scheme targeting (b)(7)(C). SA (b)(7)(C) provided this information to Det. (b)(7)(C) for use in his investigation and criminal case against (b)(7)(C) (Exhibit 8).

A review of (b)(7)(C) telephone logs also revealed that she had telephone conversations with a known criminal associate of (b)(7)(C) four times prior to the January burglary using her USPS work telephone. SA (b)(7)(C) provided this information to Det. (b)(7)(C) for use in his investigation and criminal case against (b)(7)(C) (Exhibit 9).

Allegation 2: (b)(7)(C) had a prior criminal arrest history of before she was hired by Manpower.

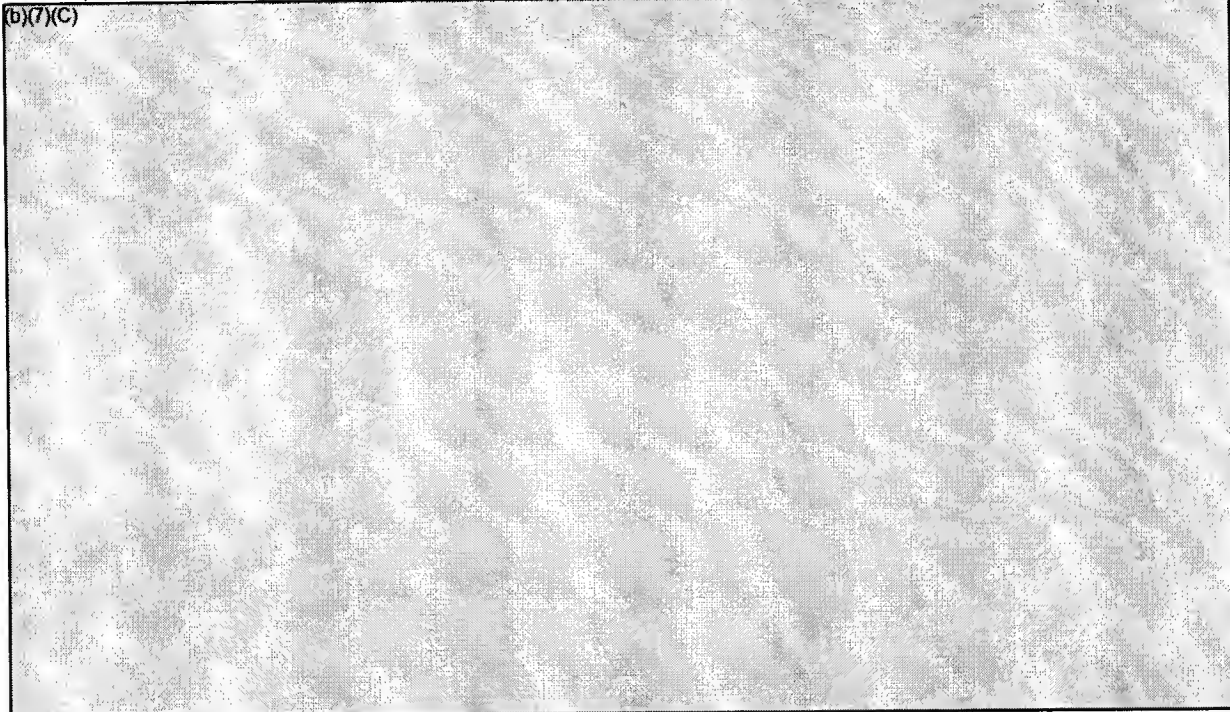
SA (b)(7)(C) reviewed a criminal history report for (b)(7)(C) which indicated she was arrested previously for felony larceny as well as for misdemeanor failing to send her child to school (truancy) (Exhibit 10).

On March 24, 2008, SA (b)(7)(C) issued an OIG Subpoena Duces Tecum to Manpower for (b)(7)(C) pre-employment, hiring and work assignment records. A review of the subpoenaed records from Manpower indicated that the USPS does not request that

contractors require employees to disclose past arrest information on their criminal history declarations. Therefore, (b)(7)(C) previous arrest history was not noted on her application to Manpower or the background forms submitted to the USPS (Exhibits 11, 12).

Allegation 3: Manpower continued to employ (b)(7)(C) after learning that she failed to disclose her arrest in February 2008, stemming from three felony theft and stolen property charges.

On March 10, 2008, SA (b)(7)(C) interviewed (b)(7)(C) Branch Manager, Manpower, Springfield, VA, regarding (b)(7)(C)



On March 28, 2008, SA (b)(7)(C) interviewed (b)(7)(C) again as a follow-up to an OIG subpoena that was issued to Manpower on March 24, 2008. (b)(7)(C) said she received the OIG subpoena for records related to (b)(7)(C) employment with Manpower. (b)(7)(C) said she engaged her Legal Affairs office to assist in preparing the OIG subpoena results. SA (b)(7)(C) asked about the status of (b)(7)(C) employment and whether Manpower had terminated (b)(7)(C) from the company. (b)(7)(C) said (b)(7)(C) is still registered with Manpower, meaning that she is still available for assignment. (b)(7)(C) declined to comment on whether Manpower has assigned (b)(7)(C) to work at another location at this time. SA (b)(7)(C) asked (b)(7)(C) why Manpower had not initiated

termination proceedings against (b)(7)(C) based on her recent arrests. (b)(7)(C) said she needed to find out who in Human Resources or Legal Affairs would be best to answer that question (Exhibit 14).

On April 9, 2008, SA (b)(7)(C) interviewed (b)(7)(C) Corporate Counsel, Manpower, Milwaukee, WI, regarding (b)(7)(C)

(b)(7)(C)

(b)(7)(C) said (b)(7)(C) was still an "associate" of Manpower, which means that she is available for assignment at other job locations. (b)(7)(C) confirmed that Manpower would not assign (b)(7)(C) to another USPS site; however, (b)(7)(C) said Manpower did not intend to fire (b)(7)(C) at this time. (b)(7)(C) said several times that (b)(7)(C) is merely charged with crimes, and that these are simply allegations. (b)(7)(C) said normally when an associate is accused of crimes involving theft or similar dishonesty, Manpower will seek work opportunities for that person at locations where it is less likely that they will have the opportunity to commit such crimes, such as product assembly work.

(b)(7)(C) said Manpower does not disclose to potential employers that the associate is currently facing criminal charges. (b)(7)(C) said in the case of (b)(7)(C) if she was assigned to another agency, Manpower is under no obligation to notify that employer of her current criminal charges. (b)(7)(C) said that even if (b)(7)(C) was convicted, she might still be able to keep working for Manpower.

(b)(7)(C) said that Manpower does not ask its associates whether they are currently facing criminal charges, only whether they have been convicted of crimes. (b)(7)(C) said in certain states, it is illegal for Manpower to ask associates whether they had ever been arrested before, assuming they were not convicted. In addition, (b)(7)(C) said certain states prohibit Manpower from disclosing that an associate is facing criminal charges.

When asked how she would characterize the removal of (b)(7)(C) from the USPS contract, (b)(7)(C) said, (b)(7)(C) access to the USPS facilities was terminated on (b)(7)(C) as far as Manpower is concerned." (b)(7)(C) said Manpower would be sure

never to reassign (b)(7)(C) to another USPS contract. As it relates to (b)(7)(C) pending criminal charges, SA (b)(7)(C) provided (b)(7)(C) with the contact information for the Fairfax County Clerk of Courts (Exhibit 15).

V. DISPOSITION

Investigative activity by the OIG has concluded and all relevant information was provided to the Fairfax County Police Department. This Report of Investigation is prepared as an investigative summary for the official case file. (b)(7)(C) is scheduled to appear at Fairfax County Circuit Court for trial in July 2008.

VI. EXHIBITS

1. Case Initiation, dated March 4, 2008.
2. Memorandum of Activity, Contact with Det. (b)(7)(C) dated March 7, 2008.
3. Felony charge 1 of 3 against (b)(7)(C)
4. Felony charge 2 of 3 against (b)(7)(C)
5. Felony charge 3 of 3 against (b)(7)(C)
6. Memorandum of Activity, OIG notification to USPS management, dated March 9, 2008.
7. Memorandum of Activity, Seizure of two USPS computers, dated March 9, 2008.
8. Forensic Lead Closure, Web Logs, dated March 10, 2008.
9. Memorandum of Activity, Analysis of USPS telephone logs, dated April 15, 2008.
10. Criminal History for (b)(7)(C)
11. OIG subpoena to Manpower, issued March 24, 2008.
12. Manpower response to OIG subpoena, dated April 7, 2008.
13. Memorandum of Interview, (b)(7)(C) dated March 10, 2008.
14. Memorandum of Interview, (b)(7)(C) dated March 28, 2008.
15. Memorandum of Interview, (b)(7)(C) dated April 9, 2008.

EMBEDDED EXHIBITS

1. Case Initiation, dated March 10, 2008.

CI - (b)(7)(C) - 3-10-2008

2. Memorandum of Activity, Contact with Det. (b)(7)(C) dated March 7, 2008.

Contact with Fairfax PD - Det (b)(7)(C)

3. Felony charge 1 of 3 against (b)(7)(C)

Felony Larceny - credit cards - Fairfax County GDC

4. Felony charge 2 of 3 against (b)(7)(C)

Felony Larceny - credit cards - charge 2 - Fairfax Co GDC

5. Felony charge 3 of 3 against (b)(7)(C)

Felony Larceny - credit cards - charge 2 - Fairfax Co GDC

6. Memorandum of Activity, OIG notification to USPS management, dated March 9, 2008.

Contact with VP (b)(7)(C) arrest

7. Memorandum of Activity, Seizure of two USPS computers, dated March 9, 2008.

Seizure of two computers for (b)(7)(C)

8. Forensic lead Closure, Web Logs, dated March 10, 2008.

Forensic Lead Closure-WebLog Analysis

9. Memorandum of Activity, Analysis of USPS telephone logs, dated April 15, 2008.

Analysis of telephone logs with known associates

10. Criminal History for (b)(7)(C)

(b)(7)(C) - previous arrests noted

11. OIG subpoena to Manpower, issued March 24, 2008.

OIG subpoena to Manpower

12. Manpower response to OIG subpoena, dated April 7, 2008.

Manpower subpoena return for (b)(7)(C)

13. Memorandum of Interview, (b)(7)(C) dated March 10, 2008.

Interview of (b)(7)(C) Manpower Branch Mgr

14. Memorandum of Interview, (b)(7)(C) dated March 28, 2008.

MOI - Interview of (b)(7)(C) (2nd) 3.28.08

15. Memorandum of Interview, (b)(7)(C) dated April 9, 2008.

Interview of (b)(7)(C) Manpower Corp Counsel

#1116



OFFICE OF THE INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 9, 2008

The Honorable Gus M. Bilirakis
U.S. House of Representatives
Washington, DC 20515

Attention: (b)(6); (b)(7)(C)

Dear Mr. Bilirakis:

We received your February 5 letter on behalf of your constituent, (b)(7)(C) alleged his home address was submitted for a change-of-address (COA) request online through the Postal Service's website without his consent. He further alleged someone attempted to steal his identity by attempting to open credit cards in his name.

We conducted an investigation, which included interviews and a review of records and documents. We found no evidence of misconduct or illegal activity by postal employees. We did determine someone external to the Postal Service submitted a COA request under (b)(7)(C) name. This is outside the jurisdiction of the Office of Inspector General, therefore, we have referred our findings to the U.S. Postal Inspection Service for investigative considerations. (b)(7)(C) stated he has not incurred any loss or damage because of this incident. Additionally, we have referred our findings to our Office of Audits for consideration of any reviews they may undertake regarding the Internet part of the Postal Service's change-of-address service.

As information, the Postal Service offers millions of Americans who move annually three methods of forwarding their mail. In addition to submitting a hardcopy Form 3575 at the post office, or by telephone, customers can now submit a COA request online at www.usps.com. Customers need to have a valid credit card for identity verification and security. A nominal fee is charged. The Postal Service is careful to take steps to ensure the COA is authorized, and to protect individuals' privacy and security. Once the application is received by the Postal Service, the customer is notified through the standard COA confirmation process. First, a move validation letter is sent to the old address indicating the request to forward mail. Secondly, a confirmation letter is sent to the new address. In both cases, if the address change is unauthorized or incorrect, the customer is advised to call 1-800-ASK-USPS.

1735 N LYNN STREET
ARLINGTON, VA 22209-2020
(703) 248-2100
FAX: (703) 248-4626

As a result, we have concluded our investigation and plan no further work on this matter. If you or your staff have any questions related to your inquiry, please contact our Director of Congressional Response, (b)(7)(C) at (703) 248-2100.

Sincerely,

(b)(6), (b)(7)(C)

Lance Carrington
Deputy Assistant Inspector General
for Investigations



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL
SOUTHEAST AREA FIELD OFFICE
TAMPA SUB-OFFICE
5201 W. SPRUCE STREET, ROOM 224
TAMPA, FL 33609**

CASE #: 08UITA3531GC04GC

CROSS REFERENCE #:

**TITLE: IDENTITY THEFT
(CONGRESSIONAL) #1116-0**

CASE AGENT (if different from prepared by): SA (b)(7)(C)

REPORT OF INVESTIGATION

PERIOD COVERED: FROM February 27, 2008 to May 21, 2008

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES:

N/A

DISTRIBUTION:

N/A

PREPARED BY: ACTING ASAC (b)(7)(C)

DATE: 05/29/2008

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

I. PREDICATION

On February 27, 2008, the U.S. Postal Service (USPS), Office of Inspector General (OIG) received an inquiry from the office of Gus Bilirakis, U.S. Congressman, Ninth Congressional District, State of Florida. The complainant, postal customer (b)(7)(C) New Port Richey, FL 34653, reported that sometime in December 2007, his home address was submitted for a change of address (COA) online through the Postal Service's website to (b)(7)(C) Brooklyn, NY, 11213-1471 without his consent. (b)(7)(C) further reported that subsequently someone attempted to steal his identity by attempting to open credit cards in his name.

II. SYNOPSIS

Investigation was unable to determine who submitted a COA online through the Postal Service's website to (b)(7)(C) Brooklyn, NY, 11213-1471 without his consent.

III. BACKGROUND

The Postal Service offers the 45 million Americans who move annually three methods of forwarding their mail. In addition to submitting a hardcopy form at the post office, or by telephone, now customers can submit a change of address request online at usps.com. Customers need to have a valid credit card for identity verification and security. A nominal fee is charged. The Postal Service is careful to take steps to ensure the COA is authorized, and to protect individuals' privacy and security. Once the application is received by the Postal Service, the customer will be notified through the standard change-of-address confirmation process. First, a move validation letter will be sent to the old address indicating the request to forward mail. Then, a confirmation notification letter will be sent to the new address. In both cases, if the address change is unauthorized or incorrect, the consumer is advised to call 1-800-ASK-USPS.

IV. SUPPORTING DETAILS:

Allegation 1

Unknown person(s) submitted a COA online through the Postal Service's website to (b)(7)(C) Brooklyn, NY, 11213-1471 without (b)(7)(C) consent. Subsequently, someone attempted to steal (b)(7)(C) identity by attempting to open credit cards in his name.

Allegation 1 Findings

On February 27, 2008, Special Agent (SA) (b)(7)(C) spoke with (b)(7)(C) Supervisor, New Port Richey Post Office by telephone regarding the COA for (b)(7)(C) (b)(7)(C) New Port Richey, FL. (b)(7)(C) reported the COA had been submitted online. According to (b)(7)(C) no COA form existed. However, (b)(7)(C) stated there should be a record of the credit card used in the transaction. A copy of the online record of the COA is attached as (Exhibit 1).

On February 28, 2008, SA (b)(7)(C) interviewed (b)(7)(C) regarding his Congressional complaint. (b)(7)(C) stated he never changed his address. Sometime in December 2007, he received a notice that his mail would be forwarded to an address in Brooklyn, NY. He immediately called the New Port Richey Post Office and the change of address was stopped. (b)(7)(C) does not know anyone in Brooklyn, NY. (b)(7)(C)

(b)(7)(C)

(b)(7)(C)

On February 28, 2008, SA (b)(7)(C) coordinated with Postal Inspector (b)(7)(C) U.S. Postal Service, Tampa, FL. (b)(7)(C) reported that the names of the residents of (b)(7)(C) Brooklyn, NY, 11213-1471 where (b)(7)(C) mail was supposed to be forwarded were (b)(7)(C)

On March 1, 2008, a Computer Crimes Unit (CCU) analysis of the data from the Internet Change of Address (ICOA) application, determined that Verizon Wireless maintains the IP address (b)(7)(C) that was utilized for the COA.

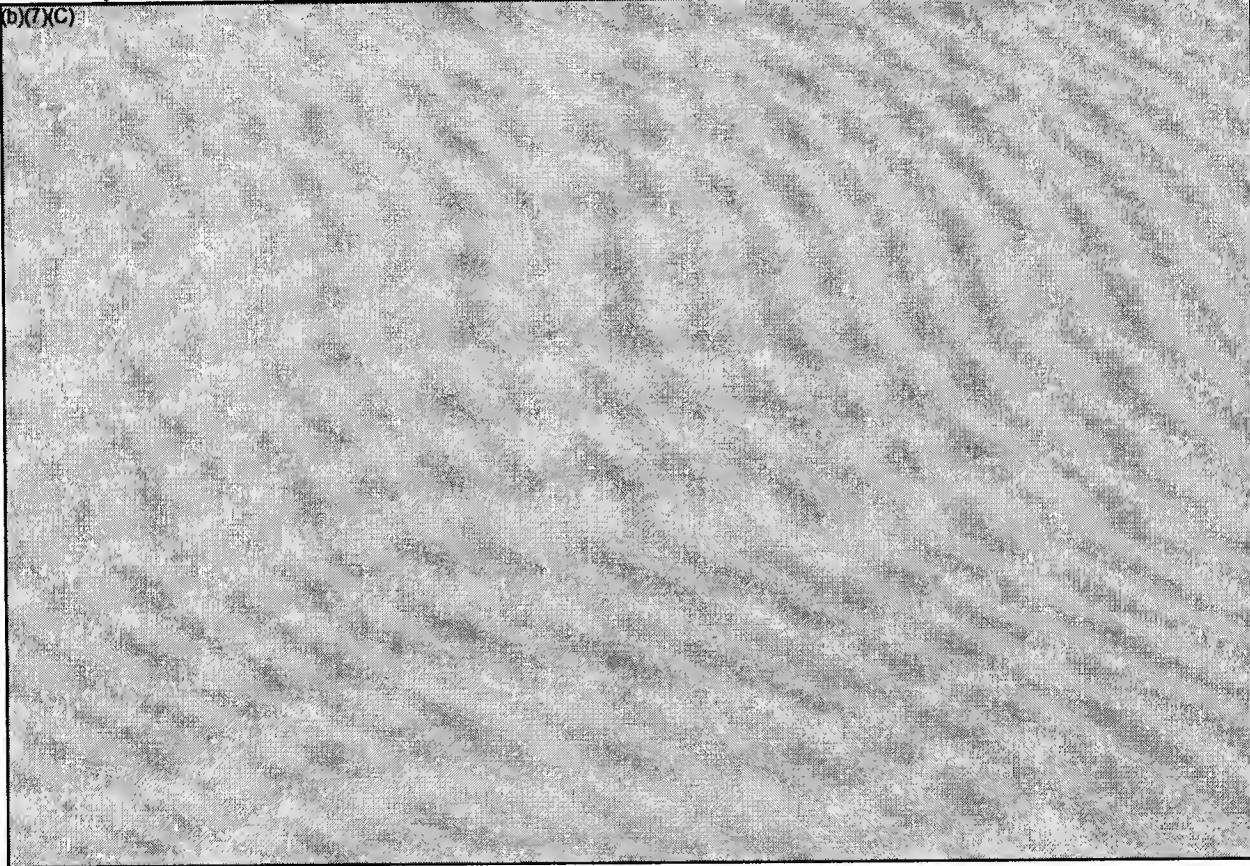
On May 14, 2008, as a result of an OIG subpoena served upon Verizon Wireless for information related to IP address (b)(7)(C) the investigation determined that the IP address belonged to Verizon Wireless customer listed as (b)(7)(C) (b)(7)(C) Brooklyn, NY 11212). Exhibit 3

On May 16, 2008, the records request submitted through Postal Service MNDDE on (b)(7)(C) did not disclose that (b)(7)(C) was a Postal Service employee (Exhibit 4).

On May 16, 2008, the Reporting Agent (RA) (b)(7)(C) conducted a database search on (b)(7)(C) within (b)(7)(C) which disclosed (b)(7)(C) currently resides at (b)(7)(C) Kissimmee, FL 34746 (Exhibit 5).

On May 19, 2008, the RA coordinated with Postal Inspector/Team Leader (b)(7)(C) U.S. Postal Inspection Service, Orlando, FL who advised that they had no ongoing or previous investigative activity pertaining to (b)(7)(C).

On May 21, 2008, the RA interviewed (b)(7)(C)



On May 21, 2008, the records request submitted through Postal Service MNDDE failed to disclose that (b)(7)(C) were Postal Service employees (Exhibit 7).

V. DISPOSITION:

Investigation determined that there were no Postal Service employees involved in (b)(7)(C) online change of address or identity theft. During the interview of (b)(7)(C) information was received that (b)(7)(C) identity was stolen in July 2007, and documented with the U.S. Postal Inspection Service (reference number #6675082). Investigation further determined that (b)(7)(C) identity theft was attempted by unknown person(s). Since (b)(7)(C) are residents of the address where (b)(7)(C) mail was to be forwarded, referral will be made to the Postal Inspection Service. Also, a referral has been made to OIG Audit for consideration of review of the Internet part of the Postal Service Change of Address service. According to (b)(7)(C) no loss or damage was incurred as a result of this incident.

EXHIBITS:

1. Change of Address effective date December 26, 2007.
2. Memorandum of Interview of (b)(7)(C) dated February 29, 2008.
3. Copy of account holder information from Verizon Wireless, dated May 9, 2008.
4. Memorandum of Activity on MNDDE on (b)(7)(C) dated May 16, 2008.
5. (b)(7)(C), (b)(7)(E) database results on (b)(7)(C) dated May 16, 2008.
6. Memorandum of Interview of (b)(7)(C) dated May 21, 2008.
7. Memorandum of Activity on MNDDE on (b)(7)(C) dated May 22, 2008.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

P. O. BOX 3478
BATON ROUGE, LA 70821-3478

CASE #: 09UIBG2958GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM April 23, 2009 TO June 26, 2009

STATUS OF CASE: CLOSED INVESTIGATION

JOINT AGENCIES:

NONE

DISTRIBUTION:

(b)(7)(C)

Maintenance Manager
1105 Moss St.
Lafayette, LA. 70501-9997

(b)(7)(C)

Plant Manager
1105 Moss St.
Lafayette, LA. 70501-9997

PREPARED BY: (b)(7)(C)

DATE: 12/02/09

Carolyn Weisiger
District Manager
Louisiana District
701 Loyola Avenue, Room 11001
New Orleans, LA. 70113-9800

(b)(7)(C)

Manager, Human Resources
Louisiana District
701 Loyola Avenue, Room 2009
New Orleans, LA. 70113-9994

(b)(7)(C)

Manager, Labor Relations
Louisiana District
701 Loyola Avenue, Room 7032
New Orleans, LA. 70113-9401

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

I. PREDICATION

In April, 2009, the United States Postal Service, Office of Inspector General Office (OIG) in Baton Rouge, La, received information regarding (b)(7)(C) (b)(7)(C) Lafayette Processing and Distribution Center. The information provided to OIG related to (b)(7)(C) committing unauthorized use of a computer. The information provided to OIG states (b)(7)(C) was seen on the postal service computer on several occasions and (b)(7)(C) has not been granted computer access with the postal service. OIG was advised that (b)(7)(C) is accessing the postal service computer using (b)(7)(C) user ID. (b)(7)(C) is a Postmaster in (b)(7)(C) Louisiana.

II. SYNOPSIS

This investigation determined that employee (b)(7)(C) did in fact use (b)(7)(C) User ID and password to gain unauthorized access to logon the postal service computer. RA obtained a printout of the logon attempts and logon successes indicating when (b)(7)(C) accessed the postal service computer using (b)(7)(C) User ID and password. The printout indicates that (b)(7)(C) accessed the postal service computer on March 7, 2009, April 3 and 4, 2009. During an interview with (b)(7)(C) she advised RA that she did provide (b)(7)(C) with her User ID and password to access the postal service computer. (b)(7)(C) advised RA that (b)(7)(C) needed to access the postal service computer to view and send emails regarding her EEO she filed against a supervisor with the postal service.

RA and S/A (b)(7)(C) interviewed (b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat 1101

(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat 1101



III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

Allegation 1: Postal Management advised that employee (b)(7)(C) has been accessing the postal service computer system without prior authorization, using another employee's User ID and password.

Allegation 1 Findings:

In April, 2009, the United States Postal Service, Office of Inspector General Office (OIG) in Baton Rouge, La, received information from (b)(7)(C) Supervisor, at the Lafayette Processing and Distribution Center, Lafayette, La. regarding (b)(7)(C). (b)(7)(C) advised OIG that (b)(7)(C) has been seen accessing the postal service computer system without prior authorization. (b)(7)(C) advised that (b)(7)(C) has not been provided computer access with the postal service. (b)(7)(C) stated he contacted the postal service Information Technology Department and was provided the User ID that (b)(7)(C) was using to access the postal service computer system. (b)(7)(C) stated the User ID belongs to another employee, (b)(7)(C) of (b)(7)(C). (b)(7)(C) stated (b)(7)(C) is employed as a postmaster with the Postal Service.

On April 20, 2009, RA contacted (b)(7)(C) Maintenance Manager regarding unauthorized computer use by employee (b)(7)(C). (b)(7)(C) advised RA that (b)(7)(C) has not been provided with a User ID or password to access the post office computers. (b)(7)(C) stated he had conversation with (b)(7)(C) about using the postal computer and (b)(7)(C) advised (b)(7)(C) that she was using (b)(7)(C) logon ID to gain access to the post office computer. (b)(7)(C) stated he advised (b)(7)(C) that there is a limited

computer use policy within the postal service. (b)(7)(C) stated (b)(7)(C) told him that she was using the post office computer to work on a school project. Memorandum of Interview with (b)(7)(C) is attached as **Exhibit #1**.

On April 23, 2009, Reporting Agent (RA) contacted S/A (b)(7)(C) Digital Evidence Services and provided S/A (b)(7)(C) with User ID (b)(7)(C) and computer ID (b)(7)(C) that was being used by (b)(7)(C). RA requested that S/A (b)(7)(C) provide RA with a review of security event log data, Internet proxy logs and internet cache from the USPS computer that was being used by (b)(7)(C).

On April 30, 2009, RA obtained from S/A (b)(7)(C) a security event log, sites visited log and Internet cache relating to User ID (b)(7)(C). The security event log indicated the number of times (b)(7)(C) attempted and successfully logged onto the postal service computer using User ID (b)(7)(C). RA noted that (b)(7)(C) logged onto the postal service computer system on three different occasions, March 7, 2009, April 3 and 4th 2009. In reviewing the sites visited log, RA noticed that all the sites visited related to Louisiana.edu in the category of education. RA noticed that there was one site relating to (b)(7)(C) in the category of Computer/Internet. Information obtained by RA indicates that (b)(7)(C) is a part of Microsoft help system which attempts to locate an application to open a file. Security event log is attached as **Exhibit #2**. Sites visited log is attached as **Exhibit #3**.

On June 16, 2009, RA and S/A (b)(7)(C) responded to (b)(7)(C) and met with employee (b)(7)(C). SA (b)(7)(C) and RA identified themselves to Johnson as Special Agents with the United States Postal Service, Office of Inspector General. RA advised (b)(7)(C) that he needed to speak with her regarding an ongoing investigation relating to misuse of a post office computer.

(b)(7)(C); (b)(3):Pub. L. No. 95-452 92 Stat. 1101

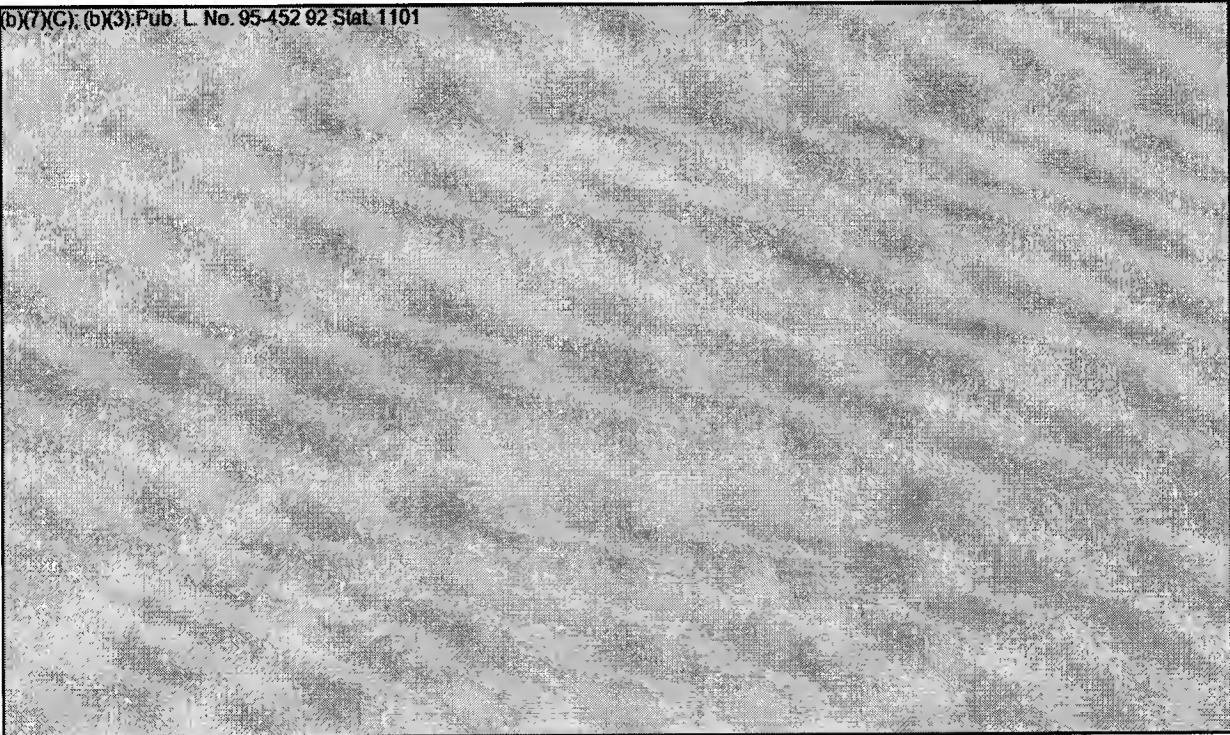


(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat. 1101

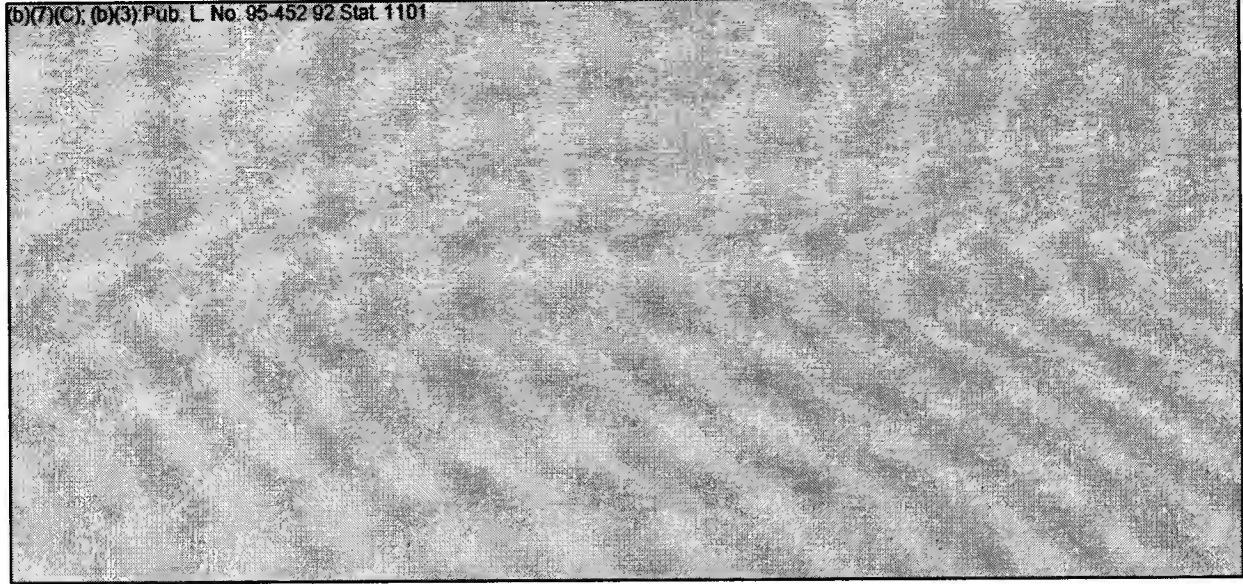


On June 16, 2009, Special Agent (b)(7)(C) and Reporting Agent (RA) responded to (b)(7)(C) and met with employee (b)(7)(C). SA (b)(7)(C) and RA identified themselves to (b)(7)(C) as Special Agents with the United States Postal Service, Office of Inspector General. RA advised (b)(7)(C) that he needed to speak with her regarding an ongoing investigation relating to misuse of a post office computer.

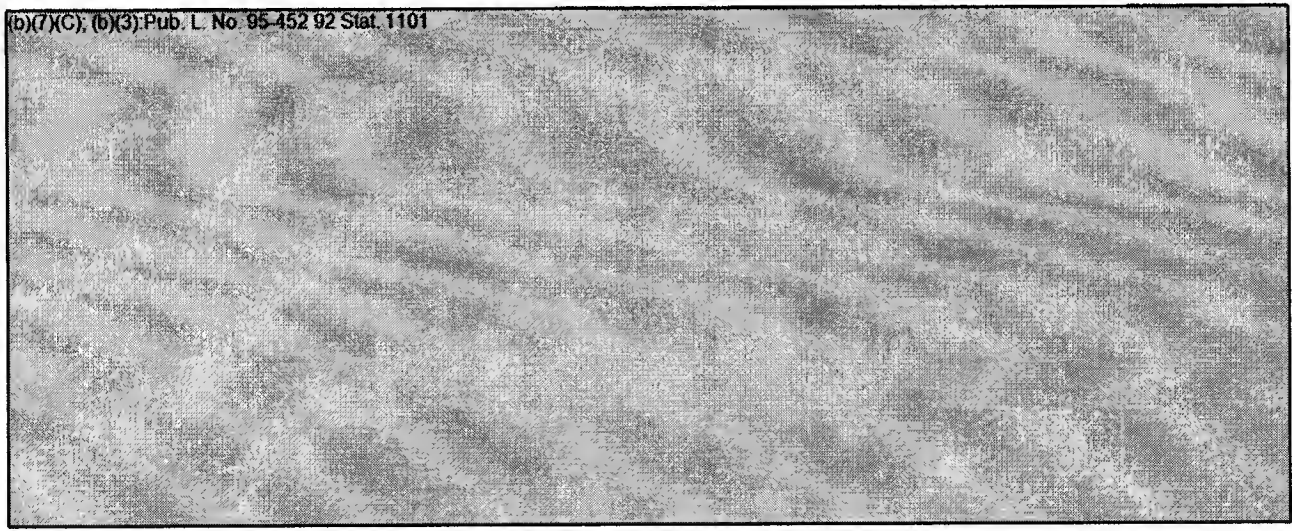
(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat. 1101



(b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101



On June 26, 2009, Reporting Agent (RA) contacted via telephone (b)(7)(C) Information Technology Specialist with USPS, in Lafayette, La. RA advised (b)(7)(C) that RA was conducting an investigation into employee (b)(7)(C) computer use. (b)(7)(C) provided the following information.



V. DISPOSITION

The Report of Investigation along with attachments is presented to USPS Management and Labor Relations for administrative action as deemed appropriate.

On December 1, 2009, Postal Management sent an email confirming (b)(7)(C) official discussion was conducted on August 18, 2009. No further action taken by Postal. This investigation is being closed.

VI. EXHIBITS

1. Memorandum of Interview with Maintenance Manager, (b)(7)(C)
(b)(7)(C)
2. Security Event Log provided by S/A (b)(7)(C) relating to User ID (b)(7)(C) indicating logon attempts and successful logons by (b)(7)(C)
(b)(7)(C)
3. Listing of Web pages visited provided by S/A (b)(7)(C) relating to User ID (b)(7)(C)
(b)(7)(C)
4. (b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101 Garrity Rights Form.
(b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101
5. Memorandum of interview with (b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101
(b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101
6. (b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101 Garrity Rights Form.
(b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101
7. Memorandum of Interview with (b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101
(b)(7)(C); (b)(3): Pub. L. No. 95-452 92 Stat. 1101

8. Memorandum of Interview with (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL
SOUTHWEST AREA FIELD OFFICE
P. O. BOX 3478
BATON ROUGE, LA 70821-3478**

June 30, 2009

(b)(7)(C)

Maintenance Manager
1105 Moss St.
Lafayette, LA. 70501

SUBJECT: Report of Investigation of (b)(7)(C)

REFERENCE: Case No: 09UIBG2958GC04GC

RESTRICTED INFORMATION

The United States Postal Service, Office of Inspector General (OIG) recently conducted an investigation pertaining to (b)(7)(C) Lafayette Processing and Distribution Center, Lafayette, LA. The Report of Investigation is enclosed for your review to determine whether disciplinary action is appropriate. Please provide your written decision within **30 days**.

The Report of Investigation is "Restricted Information". All OIG reports are furnished on an official need to know basis and must be protected from dissemination that may compromise the best interest of the Postal Service. Please do not disseminate this report without USPS-OIG authorization.

If you have any questions or need additional information, please contact Special Agent (b)(7)(C) or Assistant Special Agent in Charge

Chris Cave at (b)(7)(C)

(b)(6), (b)(7)(C)

Chris H. Cave
Assistant Special Agent in Charge
Southwest Area Field Office
Louisiana District



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

P. O. BOX 3478
BATON ROUGE, LA 70821-3478

CASE #: 09UIBG2958GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM April 23, 2009 TO June 26, 2009

STATUS OF CASE: CLOSED PENDING (ADMINISTRATIVE)

JOINT AGENCIES:

NONE

DISTRIBUTION:

(b)(7)(C)

Maintenance Manager
1105 Moss St.
Lafayette, LA. 70501-9997

(b)(7)(C)

Plant Manager
1105 Moss St.
Lafayette, LA. 70501-9997

PREPARED BY: S/A (b)(7)(C)

DATE: 06/26/2009

Page 1

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

Carolyn Weisiger
District Manager
Louisiana District
701 Loyola Avenue, Room 11001
New Orleans, LA. 70113-9800

(b)(7)(C)

Manager, Human Resources
Louisiana District
701 Loyola Avenue, Room 2009
New Orleans, LA. 70113-9994

(b)(7)(C)

Manager, Labor Relations
Louisiana District
701 Loyola Avenue, Room 7032
New Orleans, LA. 70113-9401

--	--

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

RESTRICTED INFORMATION

This report is furnished on an official need to know basis and must be protected from dissemination which may compromise the best interests of the U.S. Postal Service Office of Inspector General. This report shall not be released in response to a Freedom of Information Act or Privacy Act request or disseminated to other parties without prior consultation with the Office of Inspector General. Unauthorized release may result in criminal prosecution.

I. PREDICATION

In April, 2009, the United States Postal Service, Office of Inspector General Office (OIG) in Baton Rouge, La, received information regarding (b)(7)(C) (b)(7)(C) Lafayette Processing and Distribution Center. The information provided to OIG related to (b)(7)(C) committing unauthorized use of a computer. The information provided to OIG states (b)(7)(C) was seen on the postal service computer on several occasions and (b)(7)(C) has not been granted computer access with the postal service. OIG was advised that (b)(7)(C) is accessing the postal service computer using (b)(7)(C) user ID. (b)(7)(C) is a Postmaster in (b)(7)(C) Louisiana.

II. SYNOPSIS

This investigation determined that employee (b)(7)(C) did in fact use (b)(7)(C) User ID and password to gain unauthorized access to logon the postal service computer. RA obtained a printout of the logon attempts and logon successes indicating when (b)(7)(C) accessed the postal service computer using (b)(7)(C) User ID and password. The printout indicates that (b)(7)(C) accessed the postal service computer on March 7, 2009, April 3 and 4, 2009. During an interview with (b)(7)(C) she advised RA that she did provide (b)(7)(C) with her User ID and password to access the postal service computer. (b)(7)(C) advised RA that (b)(7)(C) needed to access the postal service computer to view and send emails regarding her EEO she filed against a supervisor with the postal service.

RA and S/A (b)(7)(C) interviewed (b)(7)(C), (b)(3):Pub. L. No. 95-452 92 Stat. 1101

(b)(7)(C), (b)(3):Pub. L. No. 95-452 92 Stat. 1101

III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

Allegation 1: Postal Management advised that employee (b)(7)(C) has been accessing the postal service computer system without prior authorization, using another employee's User ID and password.

Allegation 1 Findings:

In April, 2009, the United States Postal Service, Office of Inspector General Office (OIG) in Baton Rouge, La, received information from (b)(7)(C) Supervisor, at the Lafayette Processing and Distribution Center, Lafayette, La. regarding (b)(7)(C). (b)(7)(C) advised OIG that (b)(7)(C) has been seen accessing the postal service computer system without prior authorization. (b)(7)(C) advised that (b)(7)(C) has not been provided computer access with the postal service. (b)(7)(C) stated he contacted the postal service Information Technology Department and was provided the User ID that (b)(7)(C) was using to access the postal service computer system. (b)(7)(C) stated the User ID belongs to another employee, (b)(7)(C). (b)(7)(C) stated (b)(7)(C) is employed as a postmaster with the Postal Service.

On April 20, 2009, RA contacted (b)(7)(C) Maintenance Manager regarding unauthorized computer use by employee (b)(7)(C). (b)(7)(C) advised RA that (b)(7)(C) has not been provided with a User ID or password to access the post office computers. (b)(7)(C) stated he had conversation with (b)(7)(C) about using the postal computer and (b)(7)(C) advised (b)(7)(C) that she was using (b)(7)(C) logon ID to gain access to the post office computer. (b)(7)(C) stated he advised (b)(7)(C) that there is a limited

computer use policy within the postal service. (b)(7)(C) stated (b)(7)(C) told him that she was using the post office computer to work on a school project. Memorandum of Interview with (b)(7)(C) is attached as **Exhibit #1**.

On April 23, 2009, Reporting Agent (RA) contacted S/A (b)(7)(C) Digital Evidence Services and provided S/A (b)(7)(C) with User ID (b)(7)(C) and computer ID (b)(7)(C) that was being used by (b)(7)(C). RA requested that S/A (b)(7)(C) provide RA with a review of security event log data, Internet proxy logs and internet cache from the USPS computer that was being used by (b)(7)(C).

On April 30, 2009, RA obtained from S/A (b)(7)(C) a security event log, sites visited log and Internet cache relating to User ID (b)(7)(C). The security event log indicated the number of times (b)(7)(C) attempted and successfully logged onto the postal service computer using User ID (b)(7)(C). RA noted that (b)(7)(C) logged onto the postal service computer system on three different occasions, March 7, 2009, April 3 and 4th 2009. In reviewing the sites visited log, RA noticed that all the sites visited related to Louisiana.edu in the category of education. RA noticed that there was one site relating to (b)(7)(C) in the category of Computer/Internet. Information obtained by RA indicates that (b)(7)(C) is a part of Microsoft help system which attempts to locate an application to open a file. Security event log is attached as **Exhibit #2**. Sites visited log is attached as **Exhibit #3**.

On June 16, 2009, RA and S/A (b)(7)(C) responded to (b)(7)(C) and met with employee (b)(7)(C). SA (b)(7)(C) and RA identified themselves to (b)(7)(C) as Special Agents with the United States Postal Service, Office of Inspector General. RA advised (b)(7)(C) that he needed to speak with her regarding an ongoing investigation relating to misuse of a post office computer.

(b)(7)(C); (b)(3):Pub. L. No. 95-452 92 Stat. 1101

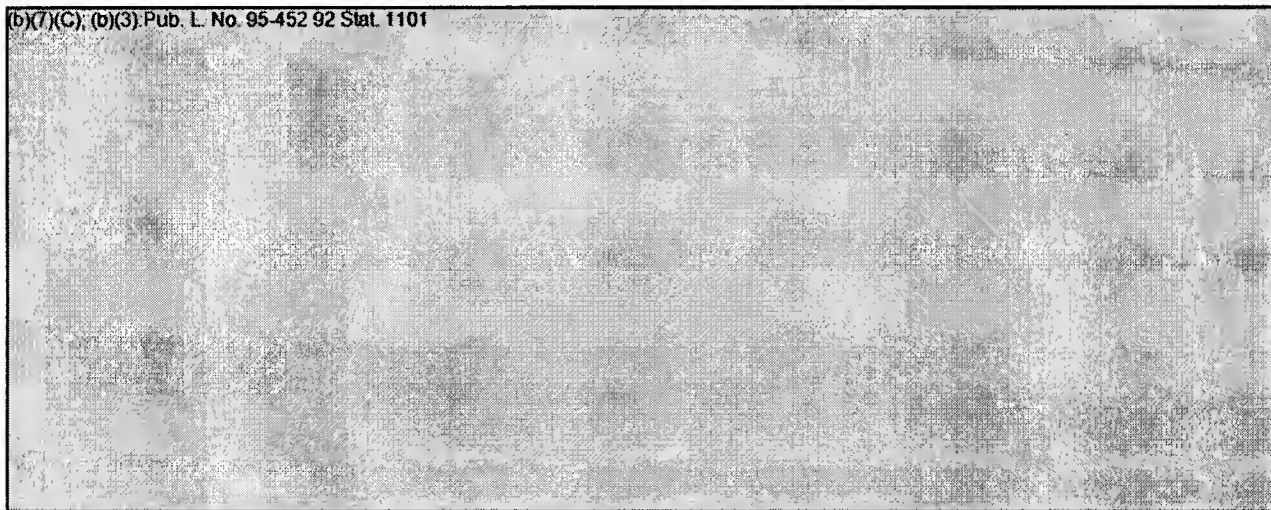
On June 16, 2009, Special Agent (b)(7)(C) and Reporting Agent (RA) responded to (b)(7)(C) and met with employee (b)(7)(C). SA (b)(7)(C) and RA identified themselves to (b)(7)(C) as Special Agents with the United States Postal Service, Office of Inspector General. RA advised (b)(7)(C) that he needed to speak with her regarding an ongoing investigation relating to misuse of a post office computer.

(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat. 1101



On June 26, 2009, Reporting Agent (RA) contacted via telephone (b)(7)(C) Information Technology Specialist with USPS, in Lafayette, La. RA advised (b)(7)(C) that RA was conducting an investigation into employee (b)(7)(C) computer use. (b)(7)(C) provided the following information.

(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat. 1101



V. DISPOSITION

The Report of Investigation along with attachments is presented to USPS Management and Labor Relations for administrative action as deemed appropriate.

VI. EXHIBITS

1. Memorandum of Interview with Maintenance Manager, (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101
2. Security Event Log provided by S/A (b)(7)(C) relating to User ID (b)(7)(C) indicating logon attempts and successful logons by (b)(7)(C)
3. Listing of Web pages visited provided by S/A (b)(7)(C) relating to User ID (b)(7)(C)
4. (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101 Garrity Rights Form.
5. Memorandum of interview with (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101
6. (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101 Garrity Rights Form.
7. Memorandum of Interview with (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat. 1101
8. Memorandum of Interview with (b)(7)(C); (b)(3) Pub. L. No. 95-452 92 Stat.



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

433 WEST HARRISON
SUITE 4000
CHICAGO, IL 60699-4000

CASE #: 09UISL0936GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

MEMORANDUM OF ACTIVITY

On September 8, 2010, (b)(7)(C) Network Distribution Center (NDC), Hazelwood, MO, 63042, stated the union has terminated all efforts to appeal (b)(7)(C) two-week suspension. (b)(7)(C) is a (b)(7)(C) at the NDC and he used his home computer to create Postal identification badges.

Since all appeals have been exhausted and all logical leads have been completed, this investigation is closed.

PREPARED BY: (b)(7)(C)

DATE: 9/13/2010



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

433 West Harrison
Suite 4000
Chicago, IL 60699-4000

December 18, 2008

Henry Dominguez
Manager, BMC
5800 Phantom Drive
Hazelwood, MO 63042-2468

Subject: Investigation into the conduct of (b)(7)(C)
St. Louis Bulk Mail Center

Reference: OIG Case No. 09UISL0936GC04GC

RESTRICTED INFORMATION

The United States Postal Service, Office of Inspector General (USPS-OIG) recently conducted an investigation of the activities of (b)(7)(C) St. Louis Bulk Mail Center. The attached Report of Investigation and exhibits are submitted for your consideration and decision as to whether disciplinary action is warranted.

Please advise me in writing within 60 days of your decision in this matter. If you decide to take disciplinary action, please furnish me a copy of the letter to the employee and your final decision letter. If arbitration or Merit System Protection Board hearings are required, the case agent will be available to testify concerning this investigation. Please advise me at least two weeks in advance of any scheduled hearings. Additionally, if your original decision is subsequently modified in any way, please advise me of the final action taken.

The Report of Investigation is "Restricted Information." All USPS-OIG reports are furnished on an official need to know basis and must be protected from dissemination that may compromise the best interest of the U.S. Postal Service.

If you have any questions or need additional information, please contact Special Agent
(b)(7)(C)

(b)(7)(C)
Special Agent
Great Lakes Area

Enclosure: Report of Investigation and Exhibits

cc: Danita Aquiningoc, Gateway District Manager
Mark R. Ott, Labor Relations Manager
James G'Sell, Manager Human Resources
Inspector (b)(7)(C) Postal Inspection Service



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

433 West Harrison
Suite 4000
Chicago, IL 60699-4000

December 18, 2008

Danita Aquiningoc
Gateway District Manager
1720 Market Street, Room 3027
St. Louis, MO 63155-9994

Subject: Investigation into the conduct of (b)(7)(C) St.
Louis Bulk Mail Center

Reference: OIG Case No. 09UISL0936GC04GC

RESTRICTED INFORMATION

The United States Postal Service, Office of Inspector General (USPS-OIG) recently conducted an investigation of the activities of (b)(7)(C) St. Louis Bulk Mail Center. Attached is an informational copy of the Report of Investigation relating to this investigation. The original Report of Investigation has been submitted to Henry Dominguez, Manager, BMC, for consideration as to whether disciplinary action is warranted.

The Report of Investigation is "Restricted Information." All USPS-OIG reports are furnished on an official need to know basis and must be protected from dissemination that may compromise the best interest of the U.S. Postal Service.

If you have any questions or need additional information, please contact Special Agent (b)(7)(C)

(b)(7)(C)

Special Agent
Great Lakes Area

Enclosure: Report of Investigation and Exhibits

cc: Henry Dominguez, Manager, BMC
Mark R. Ott, Labor Relations Manager
James G'Sell, Manager Human Resources
Inspector (b)(7)(C) Postal Inspection Service



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

433 WEST HARRISON
SUITE 4000
CHICAGO, IL 60699-4000

CASE #: 09UISL0936GC04GC

CROSS REFERENCE #: 09RSL1432

TITLE: (b)(7)(C)

CASE AGENT (if different from prepared by):

REPORT OF INVESTIGATION

PERIOD COVERED: FROM November 5, 2008 **TO** November 28, 2008

STATUS OF CASE: CLOSED PENDING (ADMINISTRATIVE)

DISTRIBUTION:

Henry Dominguez, Plant Manager, St. Louis Bulk Mail Center
Mark Ott, Gateway District Labor Relations Manager
Danita Aquiningoc, Gateway District Manager
James R. G'Sell, Gateway District Human Resources Manager
SA (b)(7)(C) U.S. Postal Inspection Service

JOINT AGENCY:

U. S. Postal Inspection Service

TABLE OF CONTENTS

- I. PREDICATION
- II. SYNOPSIS
- III. BACKGROUND
- IV. DETAILS
- V. DISPOSITION
- VI. EXHIBITS

I. PREDICATION

This case was initiated based upon information provided by Captain (b)(7)(C) Postal Police Office (PPO), St. Louis, MO, who stated the PPO received a counterfeit USPS identification badge in the mail.

II. SYNOPSIS

On November 5, 2008, (b)(7)(C) provided a counterfeit Postal Service badge, which contained the name and photograph of (b)(7)(C) St. Louis Bulk Mail Center (BMC). (b)(7)(C) advised the back of the badge contained language that stated if badge is found, please deposit in any U. S. mail receptacle or mail to: U.S. Postal Service, P. O. Box 14574, St. Louis, MO 63178-0574. (b)(7)(C) opined that someone found the badge and placed it into the mail stream, where it was forwarded to the PPO.

On November 6, 2008, (b)(7)(C) was interviewed by agents of the Office of Inspector General and U.S. Postal Inspection Service. During the interview, (b)(7)(C) admitted to making the counterfeit USPS identification badge.

III. BACKGROUND

(b)(7)(C)

IV. SUPPORTING DETAILS

On November 5, 2008, (b)(7)(C) provided a counterfeit Postal Service identification badge to the Office of Inspector General. The badge bore the name and photograph of (b)(7)(C) (Exhibit 1).

On November 6, 2008, the reporting agent and U.S. Postal Inspector (b)(7)(C) interviewed (b)(7)(C) regarding the allegedly counterfeit postal identification. (b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat 1101

(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat 1101

(b)(7)(C); (b)(3); Pub. L. No. 95-452 92 Stat 1101



V. DISPOSITION

This Report of Investigation is being provided to U.S. Postal Service management for any action deemed appropriate.

VI. EXHIBITS

1. (b)(7)(C) email and attachments
2. Memorandum of Interview of (b)(7)(C), (b)(3) Pub. L. No. 95-452 92 Stat 1101 11/6/2008



**UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL**

433 WEST HARRISON
SUITE 4000
CHICAGO, IL 60699-4000

CASE #: 09UISL2419GC04GC

CROSS REFERENCE #:

TITLE: (b)(7)(C)

(b)(7)(C) **COMPUTER THEFT OF
IDENTITY, 63155**

CASE AGENT (if different from prepared by):

CASE SUMMARY REPORT

PERIOD COVERED: FROM 03162009 TO 02222010

STATUS OF CASE: CLOSED/REFERRED TO AGENCY

SUMMARY OF INVESTIGATIVE ACTIVITY:

Investigation unable to prove suspect impersonated an Office of Inspector General Special Agent. Case discussed with an Assistant United States Attorney and declined for prosecution.

This memorandum serves to close this investigation.

PREPARED BY: (b)(7)(C)

DATE: 02222010

United States Postal Service, Office of Inspector General
FOIA Office
1735 North Lynn Street
Arlington, VA 22209-2020

August 19, 2019

This is a follow up to request number 2019-IGFP-00438:

Nothing from watchdox-mail.com was received at this address. Please resend it.

Filed via MuckRock.com
E-mail (Preferred): 75437-46472565@requests.muckrock.com

For mailed responses, please address (see note):
MuckRock News
DEPT MR 75437
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

On Aug. 16, 2019:
Subject: OIG FOIA 2019-IGFP-00438
Dear Ms. Best:

This responds to your August 16 fax to the Office of Inspector General (OIG) for a status of your June 17 Freedom of Information Act (FOIA) request for records related to 13 OIG investigation case numbers supplied by you. Due to the size of the file containing responsive documents, our response was sent via secure service Watchdox on July 30. Attached please find a copy of our final response letter for your convenience.

Please confirm @watchdox-mail.com is added to your accepted email list. You may also need to check any available SPAM folders. Please respond to this email if you still have not received our response providing a physical address where we can mail the responsive documents.

As our FOIA program continues to evolve, we are encouraging requesters to submit requests, with all attachments, via email at foia@uspsoig.gov<mailto:foia@uspsoig.gov>. Additionally, this speeds up our ability to conduct a search for responsive documents and issue our final determination. When making your FOIA request do not provide more personally identifiable information (PII) than required. Do not provide Social Security cards or numbers, or items such as birth certificates.

Sincerely,

USPS OIG FOIA Team

On July 17, 2019:

Subject: 2019-IGFP-00438, 439, 443 Best, Emma Acknowledgement

Dear Ms. Best:

Please find attached our acknowledgement of receipt for your three FOIA requests.

On July 17, 2019:

Subject: 2019-IGFP-00438, 439, 443 Best, Emma Acknowledgement

Dear Ms. Best:

Please find attached our acknowledgement of receipt for your three FOIA requests.

On June 17, 2019:

Subject: Freedom of Information Act Request: Computer - Theft of Identity (GC04)

To Whom It May Concern:

Pursuant to the Freedom of Information Act, I hereby request the following records:

Records mentioning, describing or generated as a result of the follow Computer - Theft of Identity (GC04) cases:

02UIHQ0559S3CT, 6/4/2002- 12/26/2003, in zip code 94188-2706

02UIHQ0639S3CT, 7/11/2002-12/1/2003, in zip code 30026-9360

05UIMI4153S3IO, 5/5/2005-7/13/2005, in zip code 32725

07UIBH0777CI3MS, 10/30/2006-6/6/2007, in zip code 35824

07UIGR4325CI3MS, 3/6/2007-7/10/2007, in zip code 27499

08UITA3531GC04GC, 2/29/2008-6/11/2008, in zip code 34653

08UIRF3733GC04GC, 3/10/2008-7/10/2008, in zip code 22082

08UINY3819GC04GC, 3/13/2008-4/10/2008, in zip code 07109

08UICH4504GC04GC, 4/17/2008-6/18/2008, in zip code 60540

08UIIN7062GC04GC, 8/21/2008-8/28/2008, in zip code 46201

09UISL0936GC04GC, 11/25/2008-9/13/2010, in zip code 63042

09UISL2419GC04GC, 3/17/2009-2/25/2010, in zip code 63180

09UIBG2958GC04GC, 4/23/2009-12/2/2009, in zip code 70501

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 75437-46472565@requests.muckrock.com

For mailed responses, please address (see note):

MuckRock News

DEPT MR 75437

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.